

**AN ARTIFICIAL INTELLIGENCE APPROACH
TOWARDS SEAMLESS COMMUNICATION
BETWEEN VEHICLES IN DYNAMIC ENVIRONMENT**

Thesis Submitted For the Award of the Degree of

DOCTOR OF PHILOSOPHY

in

ELECTRONICS & COMMUNICATION ENGINEERING

By

GAGAN PREET KOUR MARWAH

41800568

Supervised By

Dr. ANUJ JAIN



L LOVELY
P ROFESSIONAL
U NIVERSITY

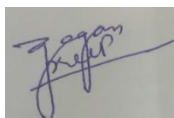
Transforming Education Transforming India

**LOVELY PROFESSIONAL UNIVERSITY
PUNJAB**

2022

DECLARATION

I, hereby declared that the presented work in the thesis entitled “An Artificial Intelligence approach towards seamless communication between vehicles in dynamic environment” in fulfilment of degree of **Doctor of Philosophy (Ph.D.)** is outcome of research work carried out by me under the supervision Dr. Anuj Jain, working as Professor, in the School of Electronics and Electrical Engineering of Lovely Professional University, Punjab, India. In keeping with general practice of reporting scientific observations, due acknowledgements have been made whenever work described here has been based on findings of other investigator. This work has not been submitted in part or full to any other University or Institute for the award of any degree.



(Signature of Scholar)

Name of the scholar: **Gagan Preet Kour Marwah**

Registration No.: **41800568**

Department/school: **School of Electronics and Electrical Engineering**

Lovely Professional University,

Punjab, India

CERTIFICATE

This is to certify that the work reported in the Ph.D. thesis entitled “An Artificial Intelligence approach towards seamless communication between vehicles in dynamic environment” submitted in fulfillment of the requirement for the reward of degree of **Doctor of Philosophy (Ph.D.)** in the Electronics & Communication Engineering, is a research work carried out by Gagan Preet Kour Marwah, (41800568), is bonafide record of her original work carried out under my supervision and that no part of thesis has been submitted for any other degree, diploma or equivalent course.



(Signature of Supervisor)

Name of supervisor: **Dr. Anuj Jain**

Designation: **Professor**

Department/school: **School of Electronics and Electrical Engineering**

University: **Lovely Professional University, Phagwara (Punjab)**

ACKNOWLEDGEMENT

High achievement always takes place in the framework of high expectation. The expectation was there and I begin with determined resolve and put in sustained hard work. It has been rightly said that every successful individual knows that his or her achievement depends on a community of persons working together but the satisfaction that accompanies the successful completion of any task would be incomplete without the mention of the people who made it possible.

*This is to acknowledge with gratitude the guidance and ameliorating suggestions from my supervisor, **Dr. Anuj Jain** for his support and motivation throughout the thesis work.*

*I am grateful to the members and Head of the Centre for Research Degree Programmes (CRDP), **Dr. Nitin Tandon** and Research Degree Evaluation Cell (RDEC), **Dr. Rekha** for being in my entire research progress review panel, providing useful suggestions during the period. I am indeed thankful to all anonymous reviewers of my research papers submitted to various International journals and International conferences, due to which I was indeed able to improve upon the work contained herein.*

I am indebted to the Honorable Chancellor, Worthy Pro-Chancellor, HOW-Research and Examination, and the successive Deans, LPU, for facilitating the administrative issues involved and encouraging me throughout.

I express my heartfelt gratitude to the Head of School, School of Electronics and Electrical Engineering, and the staff and colleagues of the School for their cooperation and support.

No words of thanks are enough to express my deepest gratitude and sincerest love to my parents, family, friends and my loving children whose rock-solid faith in me kept me strong in all circumstances.

Last but not least, I bow my head before the Almighty God for showering His mercy on me for every moment.

GAGAN PREET KOUR MARWAH

Table of Contents

Declaration.....	i
Certificate.....	ii
Abstract.....	iii
Acknowledgement.....	iv-v
Table of Contents.....	vi-x
List of Tables	xi-xii
List of Figures	xiii-xvi
List of Abbreviations	xvii-xx
 CHAPTER 1	 1
INTRODUCTION	1
1.1 Introduction.....	1
1.2. Architecture of VANETs	3
1.3. VANET routing protocols.....	6
1.3.1 Routing protocol based on topology	7
1.3.2 Position-based routing protocol	11
1.3.3. Hybrid Position-Based Routing	13
1.4. Single and Multi-hop Communications	13
1.5. Examine the VANET network's performance	15
1.6. VANET Security Attacks	15
1.7. Management of mobility.....	17
1.7.1. Frequent Handoff	18
1.7.2. Network Scenarios of Various Types	18
1.7.3. Choosing the Most Appropriate RSUs/RVs	18
1.7.4. The Multiple Access Technology Integration.....	19
1.7.5. Requirements for Different Applications.....	19
1.7.6. Issues in QoS evaluation.....	19
1.8. WSN and vehicular networks machine learning applications.....	19
1.8.1 Safety of the Network	20

1.8.2. Predicting Vehicle Movement	20
1.8.3. Accuracy	20
1.8.4. Forecasting Traffic Flows	20
1.8.5. Load Balancing on WSN	21
1.8.6. Location and Scheduling Routing	21
1.8.7. Congestion Control	21
1.8.8. Intelligent Wireless Management	21
1.8.9. Routing Techniques	22
1.9. Using artificial intelligence to secure autonomous cars	22
1.10. Techniques for Reducing Congestion	23
1.11. Routing Layer	24
1.12. VANET multi-layer challenges	24
1.12.1. Single and Dual Radio	25
1.12.2. Propagation Model	25
1.12.3. Channel Selection	25
1.12.4. Channel Estimation	25
1.12.5. Diversity Techniques	25
1.13. MAC protocol for VANET	26
1.13.1. Bandwidth Restrictions	26
1.13.2. The MAC layer: An analytical study	27
1.13.3. Contention Window (CW) dynamic adjustment	27
1.13.4. Congestion control	27
1.13.5. Synchronization	28
1.13.6. Efficient multi-channel utilization	28
1.13.7. Scheduling vs. Containment	28
1.13.8. Exposed and Hidden Terminal Issues	28
1.14. VANET Applications	28
1.15. Objectives	29
1.16. Organization of the thesis	30
CHAPTER 2	31
LITERATURE SURVEY	31
2.1 Introduction	31
2.2. Routing strategies in WSNs	31

2.3. Congestion control strategies in VANETs.....	33
2.4. Congestion control based on parameters	35
2.4.1. Adhoc Network.....	36
2.5. Routing protocols and its technical issues in VANET.....	41
2.6. Packet forwarding approaches by machine learning algorithms.....	43
2.7. Analysis of meta-heuristics optimization based malicious activity detection in VANETs	45
CHAPTER 3.....	54
MALICIOUS ACTIVITY DETECTION BASED ON DYNAMIC VANET.....	54
3.1 Introduction.....	54
3.1.1 VANET (Vehicular Ad-hoc Networks).....	54
3.2 Hybrid Meta-Heuristic Algorithm	55
3.3. Background Model.....	56
3.3.1 Firefly Optimization Algorithm	56
3.3.2. Whale Optimization algorithm (WOA)	58
3.4. Intelligent Clustering via HFWOA.....	62
3.5 Results and Discussions.....	66
3.6. Summary	77
CHAPTER 4.....	78
CONGESTION-FREE ROUTING BASED ON A DYNAMIC VANET ENVIRONMENT ..	78
4.1 Brief Introduction.....	78
4.2 Introduction to VANET Environment	78
4.2.1 Modes of VANET.....	79
4.2.2 Basic Structure of VANET	80
4.2.3 DRSC bandwidth	82
4.2.4 Dynamic clustering in VANET.....	84
4.2.5 Traffic congestion in VANET.....	85
4.3. Congestion-Free Routing Process in VANET	86
4.4. Background of QOS Routing, HHO and BWO Algorithms:.....	86
4.4.1. HHO algorithm	87
4.4.2. BWO Algorithm.....	91
4.4.3. QOS in VANET Networks	94
4.5. Hybrid-Harris Hawks-Black Widow based VANET (H-HHBW-VANET).....	96

4.6. Results and discussions.....	100
4.6.1 Performance Metrics	100
4.6.2. Performance matrices based on Node are compared	105
4.6.3. Analyze the performance matrices based on Speed.....	108
4.6.4. Comparative analysis of the performance matrices based on Speed	110
4.7. Summary	114
CHAPTER 5.....	115
A ROBUST COMMUNICATION WITH HYBRID TECHNIQUE IN VANET	115
5.1. Introduction.....	115
5.2. Improved Machine Learning in Robust Communication.....	118
5.3 Background of HHO, SVM, DDos attack.....	118
5.3.1 Harris hawk’s optimization (HHO).....	118
5.3.2. Support Vector Machine (SVM).....	121
5.3.3. Distributed denial of service (DDoS) attack	123
5.3.4 Simulated VANET	126
5.3.5 Dataset Production	127
5.4 Phase: 1- Security-based Modified SVM.....	128
5.4.1 Modified Support Vector Machine (SVM)	129
5.4.2. Selection of Optimal Kernel based on Harris Hawks Optimization (HHO)	131
5.5 Phase: 2- Reliable Resource Management using H-WDFOA-VANET.....	134
5.5.1 Hybrid WDFOA-VANET	135
5.5.2 Encircling Prey Method	135
5.5.3 Technique for Bubble-net Attacking.....	136
5.5.4 Mechanism for Encircling Shrink	136
5.5.5 Prey Search	137
5.5.6. Updating Position for Spiral	137
5.6. Results and Discussions	140
5.6.1. Dataset Description and Evaluation Metrics.....	140
5.6.2. Existing Techniques.....	142
5.6.3. Performance Metrics	142
5.6.4. Performance Analysis	143
5.6.5 Energy Consumption	145
5.6.6 Network Lifetime	147

5.6.7. Throughput.....	149
5.6.8. Packet Delivery Ratio (PDR).....	152
5.7 Summary	162
CHAPTER 6.....	164
ENSEMBLE APPROACH TO ANALYZE HYBRID METAHEURISTIC ENHANCED APPROACH TO ACHIEVE NETWORK STABILITY	164
6.1 Introduction.....	164
6.2. Literature Review.....	168
6.3. Proposed Methodology	171
6.3.1 Background model of the Seagull Optimization algorithm	171
6.3.2 Improved artificial fish swarm algorithm	176
6.3.3 Hybrid Seagull optimization and Artificial Fish Swarm Optimization.....	182
6.3.4 Existing Method.....	183
6.4 Section 1	190
6.4.1.Performance metrics	190
6.4.2. Results obtained through speed.....	195
6.5. Section 2	198
6.5.1. Parameter analysis of ANN- HFSA-VANET	199
6.5.2. Parameter analysis of Decision Tree (DT) - HFSA-VANET	200
6.5.3. Parameter analysis of Navie Bayes (NB)- HFSA-VANET	202
6.5.4. Parameter analysis of SVM.....	204
6.5.5. Parameters for analyzing different data types.....	206
6.5.6. Comparison of algorithms using parameters.....	207
6.6.Summary	209
CHAPTER 7	210
CONCLUSION AND FUTURE SCOPE.....	210
7.1. Conclusion.....	210
7.2. Future Scope.....	212
List of Publications	213
References.....	214-246

List of Tables

Chapter 2

Table 2. 1: Parameters of the congestion control of VANETs and Adhoc.....	38
Table 2. 2: Analysis of optimization based malicious activity detection in VANETs	49

Chapter 3

Table 3. 1:Node values vs Energy consumption.....	67
Table 3. 2: Node vs Drop.....	67
Table 3. 3: Node vs Throughput	69
Table 3. 4: Node vs Delay.....	70
Table 3. 5: Node vs Fairness Index.....	71
Table 3. 6: Speed vs Energy consumption.....	72
Table 3. 7: Speed values vs Drop Values	73
Table 3. 8: Speed vs Throughput	74
Table 3. 9: Speed vs Delay time	75
Table 3. 10: Speed vs Fairness Index.....	76

Chapter 4

Table 4. 1 DSRC Channel.....	83
Table 4. 2: The performance matrix of the existing method and the suggested model is built on Node	103
Table 4. 3: The performance matrices of the proposed approach and existing approach based on Speed.....	108

Chapter 5

Table 5. 1: Vehicle placement in the VANET	127
Table 5. 2: Simulation Configuration	141
Table 5. 3: performances of proposed Approaches	144
Table 5. 4: Energy Consumption based on data rate	146
Table 5. 5: Lifetime of Network	148

Table 5. 6: Throughput based data set	150
Table 5. 7: Comparison with existing approaches through nodes	153
Table 5. 8: Comparison of the proposed method to existing methods of speed	158

Chapter 6

Table 6. 1: Comparison with existing approach	191
Table 6. 2: Comparison of the proposed method to existing methods of speed	195

List of Figures

Chapter 1

Figure 1.1 Architecture of VANET	4
Figure 1.2 Topology for Routing Protocol	7
Figure 1.3 Single-hop and Multi-hop communication in VANET	14
Figure 1.4 MAC protocol of VANET	26

Chapter 3

Figure 3.1 Bubble-net feeding behaviour in humpback whales	58
Figure 3.2 (a) Shrinking encircling mechanism, (b) Spiral updating position mechanism	61
Figure 3.3 Flowchart of the HFWOA-VANET	65
Figure 3.4 Graphical representation for Energy consumption vs Node.....	67
Figure 3.5 Graphical representation for Drop vs Node.....	68
Figure 3.6 Graphical representation for Throughput vs Node	69
Figure 3.7 Graphical representation for Delay vs Node	70
Figure 3.8 Graphical representation for Fairness index (FI) vs Node	71
Figure 3.9 Graphical representation for Energy consumption vs Speed	72
Figure 3.10 Graphical representation for Drop vs Speed	73
Figure 3.11 Graphical representation for Throughput vs Speed.....	74
Figure 3.12 Graphical representation for Delay vs Speed	75
Figure 3.13 Graphical representation for Fairness Index (FI) vs Speed	76

Chapter 4

Figure 4.1 Structure of VANET.....	81
Figure 4.2 HHO algorithm phases of development	87
Figure 4.3 Patterns of prey attack by Harris hawks	88
Figure 4.4 Flowchart of BWO	91
Figure 4.5 Flowchart of H-HHBW-VANET	99
Figure 4.6 The graphical representation of Node vs Delay	105
Figure 4.7 The graphical representation of Node vs Drop.....	106
Figure 4.8 The graphical representation of Node vs Energy consumption.....	106

Figure 4.9 The graphical representation of Node vs Throughput	107
Figure 4.10 The graphical representation of Node vs Fairness Index	107
Figure 4.11 The graphical representation of Speed vs Delay	111
Figure 4.12 The graphical representation of Speed vs Drop	111
Figure 4.13 The graphical representation of Speed vs Energy consumption	112
Figure 4.14 The graphical representation of Speed vs Throughput.....	113
Figure 4.15 The graphical representation of Speed vs Fairness Index	113

Chapter 5

Figure 5.1 A widespread demonstration of the phases of the HHO	119
Figure 5.2 hyperplane supporter in SVM plane.....	122
Figure 5.3 DDoS attack.....	124
Figure 5.4 Flowchart for Proposed Methodology	125
Figure 5.5 Basic Architecture for Detection Method.....	127
Figure 5.6 Concept of Support Vector Machine (SVM).....	130
Figure 5.7 Flowchart for H-WDFOA-VANET	139
Figure 5.8 Energy consumption of proposed method.....	145
Figure 5.9 Consumption of Energy based on data set	146
Figure 5.10 Network lifetime of proposed method.....	147
Figure 5.11 Network Life-Time.....	148
Figure 5.12 Through put of proposed method	149
Figure 5.13 Plot for Throughput	150
Figure 5.14 Ratio of Packet Delivery	152
Figure 5.15 Node Vs Delay plot for proposed and existing method	155
Figure 5.16 Node Vs Drop plot for a proposed and existing method.....	155
Figure 5.17 Node Vs energy consumption plot for a proposed and existing method.....	156
Figure 5.18 Node Vs Fairness Index plot for a proposed and existing method.....	156
Figure 5.19 Node Vs Throughput plot for a proposed and existing method	157
Figure 5.20 Speed Vs Delay plot for proposed and existing method	160
Figure 5.21 Speed Vs energy consumption plot for a proposed and existing method.....	160
Figure 5.22 Speed Vs Drop plot for a proposed and existing method.....	161

Figure 5.23 Speed Vs Throughput plot for a proposed and existing method	161
Figure 5.24 Speed Vs Fairness index plot for a proposed and existing method	162

Chapter 6

Figure 6.1 Architecture of VANET	166.
Figure 6.2 Seagull Optimization algorithm	172
Figure 6.3 Flowchart of Seagull Optimization algorithm	175
Figure 6.4 Overall architecture of the proposed model	180
Figure 6.5 Flowchart for HFSA-VANET	181
Figure 6.6 Structure of CRSM	184
Figure 6.7 Architecture of Neural network	185
Figure 6.8 Mechanism structure of SVM	187
Figure 6.9 Structure of DT	189
Figure 6.10 Delay plot for a proposed and existing method	192
Figure 6.11 Energy consumption plot for a proposed and existing method	192
Figure 6.12 Drop plot for proposed and existing method	193
Figure 6.13 Throughput plot for proposed and existing method	193
Figure 6.14 Fairness Index plot for the planned and present method	194
Figure 6.15 Speed Vs Delay plot for proposed and existing method	195
Figure 6.16 Speed Vs energy consumption plot for a proposed and existing method	196
Figure 6.17 Speed Vs Drop plot for a proposed and existing method	196
Figure 6.18 Speed Vs Throughput plot for a proposed and existing method	197
Figure 6.19 Speed Vs Fairness index plot for a proposed and existing method	197
Figure 6.20 (a) Dropout ratio, (b) F1 score, (c) packet delivery ratio, (d) Throughput ratio, (e) End to end delay	200
Figure 6.21 (a) Dropout ratio, (b) F1 score, (c) packet delivery ratio, (d) Throughput ratio, (e) End to end delay	202
Figure 6.22 (a) Drop out ratio, (b) F1 score, (c) packet delivery ratio, (d) Through put ratio, (e) End to end delay	204
Figure 6.23 (a) Dropout ratio, (b) F1 score, (c) packet delivery ratio, (d) Through put ratio, (e) End to end delay	205

Figure 6.24(a) Network life time plot, (b) Energy consumption, (c) Throughput ratio, (d) Packet delivery ratio	206
Figure 6.25comparison of algorithms using parameters (a) End to End delay, (b) Packet delivery ratio, (c) Throughput ratio, (d) Drop out ratio, (e)F1 score	209

List of Abbreviations

1	WSN	Wireless Sensor Networks
2	BS	Base Stations
3	QoS	Quality of Service
4	V2I	Vehicle-to-Infrastructure
5	VANET	Vehicle ad hoc Networks
6	OBU	On Board Unit
7	RSU	Road Side Unit
8	TA	Trusted Authority
9	IBC	Intrabody Communication
10	PKI	Public Key Infrastructure
11	DSRC	Dedicated short range communication
12	TPD	Tamper Proof Device
13	GPS	Global Positioning System
14	GUI	Graphical User Interface
15	WLAN	Wireless Local Area Network
16	WIFI	Wireless Fidelity
17	V2V	Vehicle-to-Vehicle
18	V2R	Vehicle-to-Roadside
19	I2V	Inter-Vehicle
20	I2R	Inter-roadside
21	DSDV	Destination Sequenced Distance Vector
22	FSR	Fisheye State Routing
23	OLSR	Optimized Link State Routing Protocols
24	MPR	Multi-Point Relays
25	DSR	Dynamic Source Routing
26	AODV	Ad-hoc On-Demand Distance Vector
27	RREQ	Route Request
28	TORA	Temporally Ordered Routing Algorithm
29	ZRP	Zone routing protocol
30	IERP	Intra-zone routing protocol
31	DTN	Delay Tolerant Network
32	LTE	Long Term Evaluation
33	MAC	Media Access Control
34	IEEE	Institute of Electrical and Electronics Engineers
35	E2E	End to End

36	SNC	Stochastic Network Calculus
37	SQL	Structured Query Language
38	CNN	Convolutional Neural Network
39	ADAS	Advanced driving assistance systems
40	GMM	Gaussian mixture models
41	ML	Machine Learning
42	HMM	Hidden Markov Model
43	DCC	Decentralized Congestion Control
44	DCCS	Dynamic Congestion Control System
45	CSMA	Carrier Sense Multiple Access
46	STDMA	Self Organized Time Division Multiple Access
47	CSI	Channel State Information
48	EDCA	Enhanced Distributed Channel Access
49	CW	Contention Window
50	UTC	Universal Time Coordination
51	ABTTDD	African Buffalo based Two Tier Data Dissemination
52	HFWOA	Hybrid Firefly with Whale Optimization Algorithm
53	WOA	Whale Optimization algorithm
54	ACO	Ant Colony Optimization
55	PSO	Particle Swarm Optimization
56	NRC	Non-Recurrent Congestion
57	VSN	Vehicular Social Networks
58	SVM	Support Vector Machine
59	DDoS	Distributed Denial of Service
60	SDN	Software Defined Networking
61	HHO	Harris Hawks Optimization
62	CAV	Connected and Automated Vehicles
63	AFSA	Artificial Fish Swarm Algorithm
64	MPBRP	Mobility Prediction Based Routing Protocol
65	MSE	Mean Square Error
66	SOA	Seagull Optimization Algorithm
67	CRSM	Centralized Routing Scheme with Mobility
68	ANN	Artificial Neural Network
69	DT	Decision Tree
70	FOA	Firefly Optimization Algorithm
71	DEI	Dynamic Environmental Information
72		Hybrid-Harris-Hawks Black Window optimization based
	H-HHBW-VANET	VANET
73	H-WDFOA	Hybrid Whale Dragonfly Optimization

		Algorithm
74	NB	Naïve Bayes
75	AI	Artificial Intelligence
76	SCH	Service Channel
77	ERSR	Energy-Efficient Region Source Routing
78	CER-CH	Combining Cluster Head Election
79	E-SATS	Efficient and Simple Time Synchronization
80	C-ITS	Age-of-Information-Aware Decentralized Congestion Control System
81	DBSMA	Dynamic Broadcast Storm Mitigation Algorithm
82	VN	Vehicular Network
83	CDSF	Connected Dominating Set Forwarding
84	MRGM	Multimetric road guidance mechanism
85	NORAC	Non-Cooperative Beacon Rate And Awareness Control
86	ITS	Intelligent Transportation System
87	CAM	Cooperative Awareness Messages
88	PQ	Priority Queuing
89	CCC-MAC	Controlled-Coordinator-Based MAC
90	DSRC	Dedicated Short Range Communication
91	PRR	Packet Reception Rate
92	ECD	Expected Connectivity Degree
93	SDDA	Smart Directional Data Aggregation
94	QTAR	Q-learning-based Traffic-Aware Routing
95	HRA	Hybrid Routing Algorithm
96	BRFD	Bayesian-based Receiver Forwarding Decision
97	RBA	Reputation-Based Algorithm
98	UAV	Unmanned Aerial Vehicles
99	DST	Dempster–Shafer theory
100	RHR	Hybrid Routing algorithm
101	SMO	Spider Monkey Optimization
102	ECT	Entity-Centric Combined Trust
103	WHO	World health organization
104	MANET	Mobile Ad-Hoc networks
105	FI	Fairness Index
106	VN	Vehicle nodes
107	MMM	Manhattan mobility model
108	EDA	Event-driven architectures

109	BWO	Black Widow Optimization
110	CR	Cannibalism Rating
111	HFWOA-VANET	Hybrid Firefly Whale Optimization Algorithm based VANET
112	ML	Machine learning
113	RPS	Requests Per Second
114	PPS	Packets Per Second
115	RI-CS	Rider Integrated Cuckoo Search
116	ROA	Rider Optimization Algorithm
117	EHACORP	Enhanced Hybrid Ant Colony Optimization Routing Protocol
118	H-WDFOA	Hybrid Whale Dragonfly Optimization technique
119	AU	Application Units
120	HS	Hot Spots
121	V-TRADE	Vector-based Tracking Detection
122	SCARP	Stochastic Chaos based on Adaptive Routing with Prediction
123	GRU	Gated Recurrent Unit
124	GCN	Graph Convolutional Network
125	SSA	Segment Spectrum Agent
126	TA-RL	Tri-Agent Reinforcement Learning
127	IR	Intelligent Radio
128	IOT	Internet of Things
129	MPECS	Mobility Prediction-based Efficient Clustering Scheme
130	i-GMM	improved Gaussian Mixture Model
131	ASM	Attribute Selection Measure
132	HFSA-VANET	Hybrid Fish Swarm Algorithm- VANET
133	AFSO	Artificial Fish Swarm Optimization
134	H-HHBW-VANET	Hybrid-Harris Hawks Black widow optimization-based VANET

Table of Contents

Declaration.....	i
Certificate.....	ii
Abstract.....	iii
Acknowledgement.....	iv-v
Table of Contents.....	vi-x
List of Tables	xi-xii
List of Figures	xiii-xvi
List of Abbreviations	xvii-xx
 CHAPTER 1	 1
INTRODUCTION	1
1.1 Introduction.....	1
1.2. Architecture of VANETs	3
1.3. VANET routing protocols.....	6
1.3.1 Routing protocol based on topology	7
1.3.2 Position-based routing protocol	11
1.3.3. Hybrid Position-Based Routing	13
1.4. Single and Multi-hop Communications	13
1.5. Examine the VANET network's performance	15
1.6. VANET Security Attacks	15
1.7. Management of mobility.....	17
1.7.1. Frequent Handoff	18
1.7.2. Network Scenarios of Various Types	18
1.7.3. Choosing the Most Appropriate RSUs/RVs	18
1.7.4. The Multiple Access Technology Integration.....	19
1.7.5. Requirements for Different Applications.....	19
1.7.6. Issues in QoS evaluation.....	19
1.8. WSN and vehicular networks machine learning applications.....	19
1.8.1 Safety of the Network	20

1.8.2. Predicting Vehicle Movement	20
1.8.3. Accuracy	20
1.8.4. Forecasting Traffic Flows	20
1.8.5. Load Balancing on WSN	21
1.8.6. Location and Scheduling Routing.....	21
1.8.7. Congestion Control	21
1.8.8. Intelligent Wireless Management	21
1.8.9. Routing Techniques	22
1.9. Using artificial intelligence to secure autonomous cars.....	22
1.10. Techniques for Reducing Congestion.....	23
1.11. Routing Layer	24
1.12. VANET multi-layer challenges	24
1.12.1. Single and Dual Radio	25
1.12.2. Propagation Model.....	25
1.12.3. Channel Selection	25
1.12.4. Channel Estimation.....	25
1.12.5. Diversity Techniques	25
1.13. MAC protocol for VANET	26
1.13.1. Bandwidth Restrictions.....	26
1.13.2. The MAC layer: An analytical study	27
1.13.3. Contention Window (CW) dynamic adjustment.....	27
1.13.4. Congestion control	27
1.13.5. Synchronization	28
1.13.6. Efficient multi-channel utilization	28
1.13.7. Scheduling vs. Containment	28
1.13.8. Exposed and Hidden Terminal Issues.....	28
1.14. VANET Applications.....	28
1.15. Objectives	29
1.16. Organization of the thesis	30
CHAPTER 2.....	31
LITERATURE SURVEY	31
2.1 Introduction.....	31
2.2. Routing strategies in WSNs.....	31

2.3. Congestion control strategies in VANETs.....	33
2.4. Congestion control based on parameters	35
2.4.1. Adhoc Network.....	36
2.5. Routing protocols and its technical issues in VANET.....	41
2.6. Packet forwarding approaches by machine learning algorithms.....	43
2.7. Analysis of meta-heuristics optimization based malicious activity detection in VANETs	45
CHAPTER 3.....	54
MALICIOUS ACTIVITY DETECTION BASED ON DYNAMIC VANET	54
3.1 Introduction.....	54
3.1.1 VANET (Vehicular Ad-hoc Networks)	54
3.2 Hybrid Meta-Heuristic Algorithm	55
3.3. Background Model.....	56
3.3.1 Firefly Optimization Algorithm	56
3.3.2. Whale Optimization algorithm (WOA)	58
3.4. Intelligent Clustering via HFWOA.....	62
3.5 Results and Discussions.....	66
3.6. Summary	77
CHAPTER 4.....	78
CONGESTION-FREE ROUTING BASED ON A DYNAMIC VANET ENVIRONMENT ..	78
4.1 Brief Introduction.....	78
4.2 Introduction to VANET Environment	78
4.2.1 Modes of VANET.....	79
4.2.2 Basic Structure of VANET	80
4.2.3 DRSC bandwidth	82
4.2.4 Dynamic clustering in VANET.....	84
4.2.5 Traffic congestion in VANET.....	85
4.3. Congestion-Free Routing Process in VANET	86
4.4. Background of QOS Routing, HHO and BWO Algorithms:.....	86
4.4.1. HHO algorithm	87
4.4.2. BWO Algorithm.....	91
4.4.3. QOS in VANET Networks	94
4.5. Hybrid-Harris Hawks-Black Widow based VANET (H-HHBW-VANET).....	96

4.6. Results and discussions.....	100
4.6.1 Performance Metrics	100
4.6.2. Performance matrices based on Node are compared	105
4.6.3. Analyze the performance matrices based on Speed.....	108
4.6.4. Comparative analysis of the performance matrices based on Speed	110
4.7. Summary	114
CHAPTER 5.....	115
A ROBUST COMMUNICATION WITH HYBRID TECHNIQUE IN VANET	115
5.1. Introduction.....	115
5.2. Improved Machine Learning in Robust Communication.....	118
5.3 Background of HHO, SVM, DDos attack.....	118
5.3.1 Harris hawk’s optimization (HHO).....	118
5.3.2. Support Vector Machine (SVM).....	121
5.3.3. Distributed denial of service (DDoS) attack	123
5.3.4 Simulated VANET	126
5.3.5 Dataset Production	127
5.4 Phase: 1- Security-based Modified SVM.....	128
5.4.1 Modified Support Vector Machine (SVM)	129
5.4.2. Selection of Optimal Kernel based on Harris Hawks Optimization (HHO)	131
5.5 Phase: 2- Reliable Resource Management using H-WDFOA-VANET.....	134
5.5.1 Hybrid WDFOA-VANET	135
5.5.2 Encircling Prey Method	135
5.5.3 Technique for Bubble-net Attacking.....	136
5.5.4 Mechanism for Encircling Shrink	136
5.5.5 Prey Search	137
5.5.6. Updating Position for Spiral	137
5.6. Results and Discussions	140
5.6.1. Dataset Description and Evaluation Metrics.....	140
5.6.2. Existing Techniques.....	142
5.6.3. Performance Metrics	142
5.6.4. Performance Analysis	143
5.6.5 Energy Consumption	145
5.6.6 Network Lifetime	147

5.6.7. Throughput.....	149
5.6.8. Packet Delivery Ratio (PDR).....	152
5.7 Summary	162
CHAPTER 6.....	164
ENSEMBLE APPROACH TO ANALYZE HYBRID METAHEURISTIC ENHANCED APPROACH TO ACHIEVE NETWORK STABILITY	164
6.1 Introduction.....	164
6.2. Literature Review.....	168
6.3. Proposed Methodology	171
6.3.1 Background model of the Seagull Optimization algorithm	171
6.3.2 Improved artificial fish swarm algorithm	176
6.3.3 Hybrid Seagull optimization and Artificial Fish Swarm Optimization.....	182
6.3.4 Existing Method.....	183
6.4 Section 1	190
6.4.1.Performance metrics	190
6.4.2. Results obtained through speed.....	195
6.5. Section 2	198
6.5.1. Parameter analysis of ANN- HFSA-VANET	199
6.5.2. Parameter analysis of Decision Tree (DT) - HFSA-VANET	200
6.5.3. Parameter analysis of Navie Bayes (NB)- HFSA-VANET	202
6.5.4. Parameter analysis of SVM.....	204
6.5.5. Parameters for analyzing different data types.....	206
6.5.6. Comparison of algorithms using parameters.....	207
6.6.Summary	209
CHAPTER 7	210
CONCLUSION AND FUTURE SCOPE.....	210
7.1. Conclusion.....	210
7.2. Future Scope.....	212
List of Publications	213
References.....	214-246

ABSTRACT

VANETs provide self-organized vehicles with effective routing approach. However, frequent link disconnection is becoming a serious issue due to dynamic environmental changes. Therefore, the proposed work has provided four different modules of work where four types of works have been developed and successfully applied on VANET environment. Initially, the first module has introduced the hybrid metaheuristic algorithm named as HFWOA-VANET. The HFWOA-VANET has the strategy of a Firefly Optimization Algorithm (FOA) and a Whale Optimization Algorithm (WOA) that detects the malicious activity by considering the dynamic environmental information (DEI). This DEI is analyzed with the HFWOA-VANET. Consequently, the environment's harmful nodes can be isolated, and the connection link failures are prevented. Likewise, the second module has mainly focused on a process congestion-free routing for ensuring QoS parameters and it explores how QoS factors affect vehicular communication while choosing the optimal routing path. To enhance QoS for node-to-node routing, a VANET based on Hybrid-Harris-Hawks Black Window optimization (H-HHBW-VANET) method is developed. Next, the third module integrates two phases. Phase I uses SVM-HHO to identify the DDoS attack and offer details about the vehicle. Phase II utilizes a Hybrid Whale Dragonfly Optimization Algorithm to allocate bandwidth while reducing the effects of DDoS attacks (H-WDFOA). This efficient method is used for anticipating and utilizing the trustworthy data, that produces efficient results in smart vehicles. In last module, the overall performance is enhanced by using a best routing protocol that is hybrid ensemble learning and metaheuristic algorithm. Data extraction from the Road Side Unit (RSU) or the Base Station is estimated using seagull optimization and the Artificial Fish Swarm Optimization approach (BS). A number of machine learning techniques, including as Nave Bayes (NB), Support Vector Machine (SVM), Artificial Neural Network (ANN), and Decision Tree, are used to forecast the execution, and the hybrid metaheuristic algorithm and ensemble machine learning are coupled to reduce delay (DT). In order to achieve the best results, the effectiveness of machine learning algorithms may be assessed. Several performance metrics, including throughput, delay, drop, network lifetime, and energy usage, are used to analyze the performance. All four of these modules have now been integrated into the NS2 and MATLAB platforms.

CHAPTER 1

INTRODUCTION

1.1 Introduction

Wireless Sensor Networks (WSN) rely on data collection and transmission to Base Stations (BS) for further processing. WSN has attracted a lot of interest because of its capacity to provide efficient solutions in a variety of industries. It offers considerable cost and efficiency savings when it comes to identifying occurrences. WSN is made up of low-cost wireless sensor nodes that ensure precise and long-term event detection. Such sensor networks can be placed along the highway to detect, analyze, and transmit information gathered from the driving environment through sensor node collaboration. Sensor nodes, on the other hand, have severe resource constraints, including limited energy, communication range, and processing and storage capacity. Many challenges confront WSN technology, including poor quality of service (QoS), brittle vehicle-to-infrastructure and connection (V2I), channel access delay, congestion, and data packet loss.

Although a lot of effort is being undertaken to overcome the constraints of these concerns, their complexity and fast change pose a lot of questions. The diversity of applications for intelligent transportation systems, including vehicle ad hoc networks (VANETs), in smart metropolitan areas has increased thanks to the rapid and enormous growth of computer systems and wireless networks [1]. The density of traffic in metropolitan areas is increasing on a regular basis. As a result, there are more traffic jams and accidents, and the time it takes to get to one's destination grows. Adopting VANETs is primarily intended to reduce traffic accidents, save passengers' time, and provide a stress-free and enjoyable driving experience in metropolitan environments. To do this, modern wireless communication technology is used to link vehicles to roadside infrastructure and to one another. There are three main parts to a VANET. the entity containing the OBU, RSU, and Trusted Authority (TA) [2]. In terms of efficiency and security protocols, each communication system might be unique.

a) OBU

- ✓ The OBU features provided in each car may be different. Each car has a wireless communication device, such as the OBU, placed to collect information from nearby vehicles or sensors at the roadside.
- ✓ Utilizing the IBC procedure, a sender car sends a message to nearby vehicles by using PKI (Public Key Infrastructure) methodology and the RSU through the DSRC(Dedicated short-range communication) protocol.
- ✓ Each vehicle has an OBU that acts as a tamperproof device (TPD) that prevents the stored data from being accessed.
- ✓ A global positioning system (GPS) and a graphical user interface (GUI) are also included in each vehicle to give extra features to motorists and pedestrians.
- ✓ Each OBU's processing and storage capacity is lower than those of the RSU and TA in VANETs [3].

b) RSUs

- ✓ To improve vehicular traffic and supervision, RSUs transmit information within their transmission range. These are roadside points of entry that are permanently installed. They look after the vehicles as well as the TA.
- ✓ The DSRC protocol is used by every RSU to interact with and control the vehicles inside the range.
- ✓ Messages sent from vehicles that work in different conditions are authenticated by each RSU.
- ✓ In VANETs, every RSU has lower storage and distribution capabilities than the TA [4].

c) TA

- ✓ TA functions as a PKG, generating and broadcasting public process variables and registering RSUs and vehicles. It also allocates vehicle pseudo-identities to protect transmission privacy and produces secret keys for vehicles.

- ✓ Moreover, the TA manages a database that contains both genuine and fictitious vehicle IDs. The TA uses this information to decide a vehicle's true identity in the event of a disagreement.
- ✓ Particularly compared to other VANET entities, it has a lot of computational power and storage space.

1.2. Architecture of VANETs

Vehicles in a VANET connect using wireless links installed on every vehicular unit because the nodes communicate with another mobile node that is within their own communication range. Each node in VANET serves as both a participant and a router in the network. Considered to be self-nature, VANETs have no predefined architecture [5]. VANET architectural style can be divided into three categories:

- (a) Wireless Local Area Network (WLAN) that is entirely cellular.
- (b) Ad-hoc networks in their purest form.
- (c) Networks with a hybrid configuration.

The vehicle units in the cellular WLAN connect to the internet via cellular portals and WLAN access points. It aids vehicular junctions by providing traffic congestion and control information. It also offers information and entertainment services such as data downloads, breaking news, driving information, and advertisements. Due to the increasing price of cellphone towers, WIFI access points, and geographic constraints, deploying such architecture is extremely difficult. It allows automobiles to communicate with each other and with surrounding vehicles [6]. It is often referred to as a vehicle ad hoc network. This architecture gathers and disseminates road-related data without taking into account any established infrastructure. Vehicles are allowed to roam about on the road and their great mobility causes rapid changes in the existing structure. The network is fragmented due to the constant topology modifications. During purely ad-hoc configuration, frequent network breakdowns caused by the rapid mobility of vehicles and infrastructure make data routing

more difficult. The purely ad-hoc mode has the advantage of avoiding the expense of BS installation. It enables vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communication. This form of architecture aids in the delivery of information that gives us great as well as increased mobility. The architecture of VANET is seen in Figure 1.1.

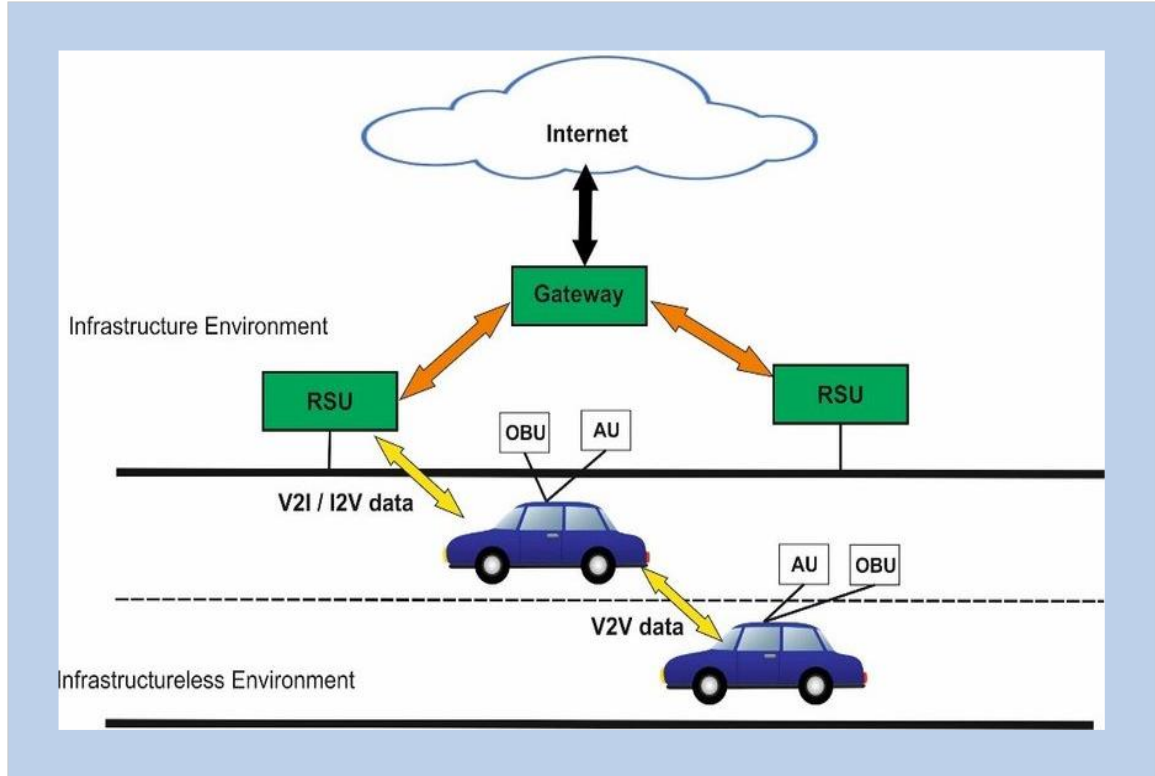


Figure 1.1: Architecture of VANET

Vehicle-to-roadside (V2R) communication, Inter-vehicle (I2V) communication and Inter-roadside (I2R) communication are the three types of VANET communication. A network in which different types of cars communicate with each other is known as an I2V communication system. The V2I and V2R protocols are used to share data between vehicles and RSUs in a vehicle-to-roadside data transmission [7]. A structure in which the RSU communicates with the BS in the range is known as an I2R communication system. Furthermore, owing to the increased node mobilities, even single-hop inter-vehicle communication is unstable and suffers from severe channel fading and shadowing issues.

Vehicles move at a fast pace. For this reason, a VANET system must be able to cope with a network where units are moving about at high rates and potentially arriving and quitting the connection at a rapid rate. Because automobiles are among the extremely fast environments where new systems are now employed, they are among the most distinguishing properties of VANETs [8]. As a result, determining whether longer a vehicle will be anticipated to remain in a connection is critical. The communication will be short if a car is traveling in the wrong manner. In this case, the system would want to send only the most critical data to limit the chances of the data being lost. If on either hand, a collection of vehicles is all going at the same moment, the connection will have a really extensive time to send any received data. Multi-hop communication becomes more difficult as a result of the high mobility, as it becomes important to determine that data packets will survive in the channel long enough to finish the required transfer. In V2I communication, on the other hand, the TA uses a Graphical User Interface to transmit some entertainment options and some other congested roads information to drivers and passengers of vehicles (GUI). Vehicles can quickly modify their route based on the information gathered in order to prevent factors that involve issues or concerns scenarios like as heavy traffic, accidents, and so on. In other words, it is typical in VANETs for senders and receivers to use various cryptographic algorithms. As a result, vehicle-to-infrastructure and vehicle-to-vehicle transmission are varied. VANETs have become a very active study subject due to the difficulties inherent with such diverse interactions in-vehicle environments [9]. Security, authenticity, stability, privacy protection, and non-repudiation are among the necessities.

The advantages listed above lead one to believe that VANETs are a revolutionary approach to contemporary traffic control. Benefits are typically accompanied by challenges. Protection of traffic-related information, vehicle confidentiality, and performance effectiveness of computational expenses are all challenges in developing VANETs. All of these things must be carefully considered. First and foremost, VANET connects various wireless networks where security is critical. An attacker can simply get access to the channels of communication and use them to collect, delete, replay, or edit traffic-related information, as well as mimic other cars. As an example, an attacker might disseminate false

traffic-related information to influence the actions of automobiles and RSUs, causing congestion or accidents. As a result, before accepting the communications, the receiver must authorize the origin of the information as well as check its integrity. In VANETs, protecting the privacy of the vehicles comes second to authorization [10]. The assailant can determine a vehicle's initial identification or even its travel itinerary using the data acquired from captured transmissions. Each vehicle must therefore have identifiable invisibility in order to guarantee privacy and unlikability. Additionally, any malicious vehicle that broadcasts false traffic-related information through VANETs must be able to be discovered and have its registration cancelled by the TA.

1.3. VANET routing protocols

Routing is the method of moving information from a sender to the receiver across a series of hops. Routing protocols are in charge of determining the route to the destination, sending packets to their destinations and forming an alternate path in the event of a failure. Proactive, reactive, and position-based routing protocols can be found among these protocols. Even though the routing path is not used, proactive routing systems keep track of routing information. Reactive routing protocols, on the other hand, execute the path discovery phase only when it is required and only keep track of routes that are currently in use. Contrarily, position-based routing protocols, require nodes to be physically located in order to promote communication [11]. The beaconing approach can be used to determine the location of neighbours, and geographical identification technologies such as GPS can be used to determine the location of a destination. Position-based routing techniques do not include route creation or management. Infrastructure-less and infrastructure-equipped routing systems are position-based routing protocols' two varieties. Routing protocols without infrastructure are further separated into simple and complex categories. We provide a brief introduction of basic routing protocols in this part, as well as a full explanation of all other protocols.

1.3.1 Routing protocol based on topology

Routing Protocols are industry standards for data transmission in networks. Routing protocols are effective to create dynamic routing optimization selections in a medium. There are two different kinds of topology-based routing protocols: proactive and reactive. Topology-based routing systems perform badly in comparison to position-based routing methods [11]. Additional node topology information is generally required by topology-based routing algorithms during the routing choice process.

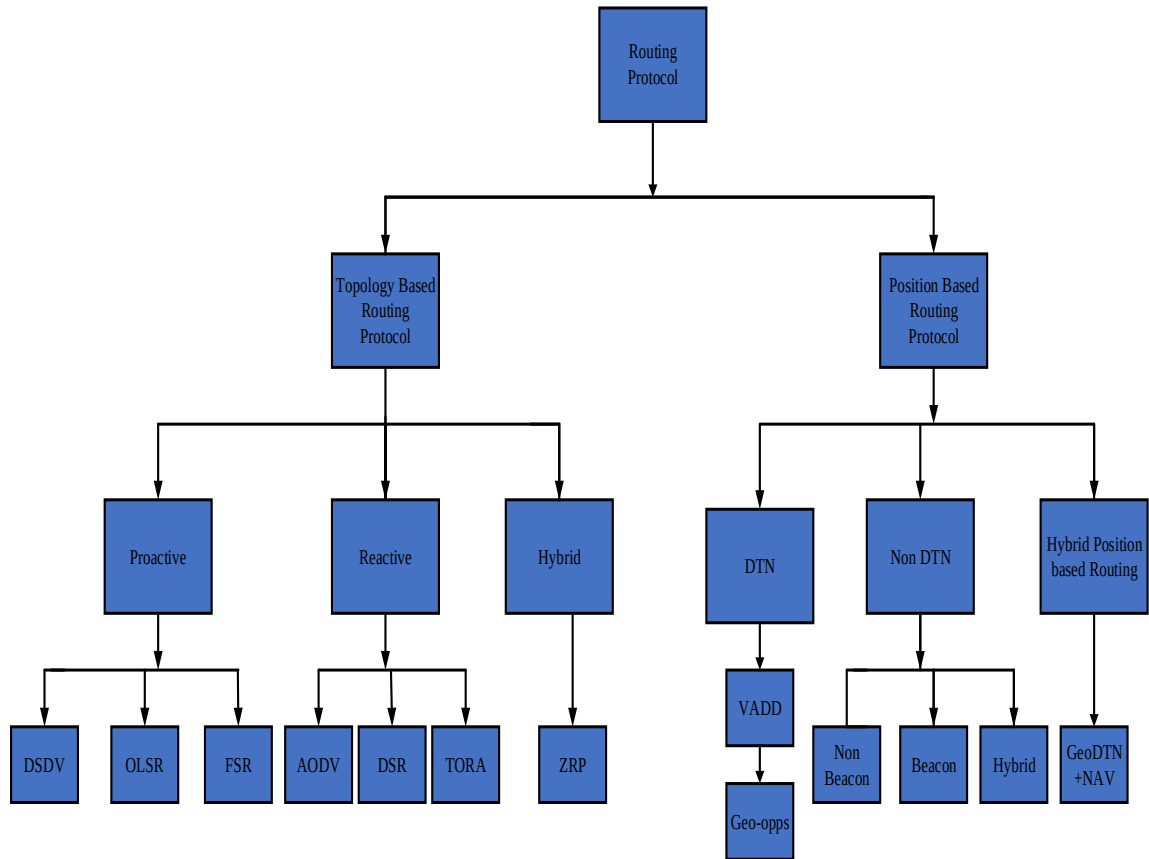


Figure 1.2: Topology for Routing Protocol

Figure 1.2 illustrates the VANET routing protocol. In the routing decision-making process, Topology Based Routing methods normally require extra node topological information.

1. Proactive Routing Protocols

Tables chosen to represent the topology are maintained by proactive routing protocols. The tables in these protocols are updated on a regular basis, and data is sent from one unit to another. Because of their nature, proactive routing protocols are often known as table-driven protocols. In proactive protocols, there seem to be two types of modification: periodic updates and triggered updates. Broadcasting update tables wastes network power and bandwidth [12]. While devices are added to connections, the table size is increased in proactive protocols, which increases the demand. The DSDV (Destination Sequenced Distance Vector) and FSR (Fisheye State Routing) protocols have been recommended as a result. Due to the overhead in routing tables, proactive protocols are not appropriate for large networks [13]. In these protocols, the shortest path methods are frequently employed.

a. Destination Sequence Distance Vector Routing (DSDV)

Loop-free pathways are made possible by Destination Sequence Distance Vector Routing (DSDV), which use the distance vector shortest path technique with a single source to destination. The protocol sends two sorts of packets: progressive and full dump. Full dump packets contain routing information, while progressive packets contain updates. Full dump packets consume more bandwidth, while progressive packets are sent more frequently, increasing network overhead. Due to bandwidth usage and update methods, the DSDV protocol is not appropriate for big networks.

b. Optimized Link State Routing Protocols (OLSR)

The term "OLSR" refers to the proactive, point-to-point Optimized Link State Routing Protocols, which are based on the established link-state algorithm. For route establishment or route maintenance, it employs a technology known as multipoint relaying, which optimizes the message and flooding process. Multi-Point Relays (MPR) [14] is an algorithm that decreases the amount of operating relays for covering the neighbours. The protocol was developed to make sure that data routing in a network was accurate and stable. Two key tenets of the OLSR are the delivery of link-state information for routing maintenance and the Multipoint Relays (MPRS) algorithm, which covers both one-hop and two-hop neighbours. Unselected packets are unable to retransmit updates, because updates

are only ever received once per node. The primary benefit of this protocol is the knowledge and recording of all routes and endpoints prior to the operation. Calculating the effective concentration, however, might be challenging in some situations because of how quickly the nodes are moving.

c. The Fisheye state routing protocol (FSR)

FSR updates system information to many other devices in the system by keeping a routing table for nodes. It is shrinking the updated message's size. For large networks, it is manageable, but the problem is scalability, and because of scaling, the precision is insufficient, leading the routing table to enlarge. When the target node is outside the scope of the source node in the FSR, the routing algorithm fails.

2. Reactive/Ad-hoc based routing

In contrast to proactive protocols, reactive protocols are unable to retain tables whenever the topology changes. The network is flooded with queries whenever a source node wishes to transfer data, and the chosen path is kept until a different node becomes inactive. They deal with the handling of route answers and cache paths. The route discovery method places a cap on the network's bandwidth. Dynamic Source Routing (DSR) and Ad-hoc On-Demand Distance Vector Routing are two popular Reactive protocols (AODV) [15].

a. On-Demand Distance Vector routing (AODV)

Demand-based reactive protocols include AODV. The DSDV and the DSR algorithms underpin AODV protocols. The protocols start the route discovery by working with routing tables. A Route Request (RREQ) packet is broadcast through the sender, and neighbour nodes pass the message on to their neighbours until an active route is found and the ideal number of hops is met during the discovery phase. Before transmitting the packet to the neighbours, the RREQ packets are unaware of the alternate path for the desired target. Many studies have concluded that AODV quality and performance are best measured by three criteria: packet loss rate, routing complexity and path optimality. The development of On Demand distance routing protocols has led to the development of new protocols including AOMDV, S-AOMDV, RAOMDV, and SD-OMDV.

b. Dynamic Source Routing Protocol (DSR)

In that it builds routes as needed and uses packet forwarding rather than tables to do so, the DSR is comparable to the AODV. DSR does not involve regular hello messages and does not use beacons [16]. DSR works by flooding route request packets into the network periodically, then requesting the route-travelled packet to be carried in the response's header by the destination node. The whole order list of networks enables packet routing while doing away with the requirement for loop-free information and current routing at intermediary nodes. The route is now included at the beginning of each packet header and other nodes forward and caching the routing for later use.

c. Temporally Ordered Routing Algorithm TORA

The Temporally Ordered Routing Protocol is a reactive and demand-driven routing protocol. In extremely dynamic Ad-hoc networks, TORA focuses on restricted control message propagation. A node in TORA clearly launches a request when it needs to transfer data to a destination. TORA activities include route maintenance, route creation from transmitter to the receiver, and route elimination when the route is no longer viable and the 3 types of signals used for these tasks are QRY for route creation, and the UPD for route development and maintenance and CLR for route elimination. When the topology changes, TORA reduces the communication overhead [17]. It performs well in dynamic Ad-hoc networks. In the network, TORA performs better than DSR.

3. Hybrid routing

Hybrid routing combines the properties of reactive and proactive protocols. The proactive functionality protects the more correct information in the local scope, whereas the reactive feature protects the more reliable information in the private network. Zone-based routing methods separate nodes into distinct zones for packet forwarding and discovery in hybrid routing protocols. A Hybrid routing system reduces total routing protocol overhead and improves efficiency in highly dynamically changing environments.

a. ZRP: Zone routing protocol

Route discovery takes place more quickly and with less overhead thanks to the Zone Routing Protocol (ZRP). Additionally, the protocol divides a group of nodes into zones that

are separate from one another and overlap, and the units are based on zone radius. The creation of the zones and their selection are based on node topological dispersion and hop distance, respectively. Peripheral nodes are those that are located on the edge of the zone. The size and radius of the zone are determined by the radius of length, which is the number of hops to the zone's boundary. Secondary nodes are in charge of determining routes outside of the zone, and a reactive intra-zone routing protocol is used to do this (IERP). Intra-zone Routing Protocol is a proactive routing method used within the domain.

1.3.2 Position-based routing protocol

Position-based routing enables multiple-hop communication in a wireless ad hoc network. In geographic routing, a node's forwarding is primarily influenced by the location of its one-hop neighbours and the location of a packet's recipient. In the headers of the packet, the location's position is recorded.

1.3.2.1. Delay Tolerant Network (DTN)

Allows for delays to combat inconsistent connectivity in urban environments, network algorithms implement various essential tasks. The carry and forward approach is used when a network node connection regularly fails. When a node is unable to communicate with other nodes, it retains packets and forwards them when it connects to an adjacent node. VADD and GeoOpps are two examples of DTN routing algorithms.

a. VADD

The query and forward premise form the foundation of VADD. One of the main challenges is selecting a forwarding method with a short packet delivery time. It adheres to some fundamental principles, such as sending the most routing data over wireless channels and choosing the quicker route when a packet needs to travel over a certain route. Dynamic path selection should be carried out continuously during the packet forwarding process since reliable packet delivery along the pre-computed best path cannot be guaranteed in vehicular ad-hoc networks due to the high chance of topology change. The VADD routing algorithm uses the intersection, straightaway, and destination procedures, in which each vehicle makes a decision at a junction and chooses the future forwarding course depending on the activities. Urban VANET environments can use VADD because it doesn't require any

infrastructure to function [18]. Both the data transmission rate and the overhead of the control packets are high. The connection is established by beacon transmissions.

b. GeoOpps

A delay-tolerant network routing system that uses GPS data to strategically route data to a target location. It selects vehicles that transport the data based on the GPS indicated routes. The closest point where they would get to the message's target is computed by neighbour vehicles chasing recommended routes to the vehicle's destination. The closet point and their map are then combined in a convenience function to explain the quickest estimated time for this message to reach at its destination. The next packet carrier is the one that can transport the packet more rapidly or closer to its destination.

1.3.2.2. Non-DTN

Non-DTN geographic routing methods are only effective in heavily populated VANETs and do not account for lost connections [19]. The local maximum refers to the situation in position-based routing where a node has no neighbours and the forwarding method fails to produce a packet. In this case, the non-DTN routing protocol develops a recovery technique to handle the failure. Hybrid, non-beacon, and beacon are the three non-DTN routing protocols.

a. Beacon

This individual category routing protocol gathers data about 1-hop or 2-hop neighbours via beacon messages. In the routing and forwarding operation, beacons often play two roles. It is used to figure out who is the closest neighbour to the endpoint and to find anchor nodes. Beacon routing methods come in two flavours: non-overlay and overlay.

b. Non beacon

A geographical routing method called Non-Beacon does not need to send out beacon frames in advance. The number of packets is transmitted to all direct neighbours, who determine whether or not to forward them. A decentralized timer-based contention algorithm selects the actual forwarder, allowing the most suited node to keep sending a packet while suppressing other prospective forwarders. The length of the final hop to the destination would be compared to the distance between the recipients of the broadcasting

data. The gap will widen, progress will accelerate, and the clock will tick faster. Contention-Depending A routing method that doesn't depend on the position of the beacon is forwarding [20].

c. Hybrid

A global routing system called hybrid minimal DTN selects the best target forwarder using 2-hop beaconing topology knowledge and combines opportunistic sending with the highest chance of success. A target node is described as a node that a greedy or restoration algorithm would typically choose, with the exception of junctions, whereby optimization in determining the destination node either beyond or depending on whether the routing is in greedy or recovery mode at the junction.

1.3.3. Hybrid Position-Based Routing

Utilizing both non-DTN and DTN routing systems, hybrid geographic routing techniques can take advantage of faulty communication lines. [21]. Position-based routing system called GeoDTN+NAV combines the greatest features of both worlds.

1.3.3.1 GeoDTN+NAV

The combination of the perimeter mode, greedy mode, and DTN mode in GeoDTN+NAV provides a combination of non-DTN and DTN routing algorithms. The GeoDTN+NAV notion is that nodes are suspected of belonging to the network and that the system is separated depending on the amount of hops packets that have moved in the perimeter. The combination of the greedy mode, perimeter mode, and DTN mode in GeoDTN+NAV provides a combination of non-DTN and DTN routing algorithms. Both the data transmission rate and the overhead for control packets are reasonable. It establishes paths using beacon messages and can employ the road obstructing propagation model.

1.4. Single and Multi-hop Communications

Alerts, accident prevention, smart route/traffic queries and other essential information can be transmitted in real-time using a single-hop or multi-hop communication network. The data can be delivered in a single-hop transmission from the sender to all accessible nodes. The data is propagated from the recipient node to other devices in the

network for multi-hops [22]. Information could also be sent to the neighbouring nodes on a regular basis. Depending on the type of message being sent and the range of communication, single-hop or multi-hop transmission is determined. Single hop transmission is recommended when a vehicle wants to communicate data to another vehicle within a short distance. Figure 1.3 depicts the VANET's single-hop and multihop communication.

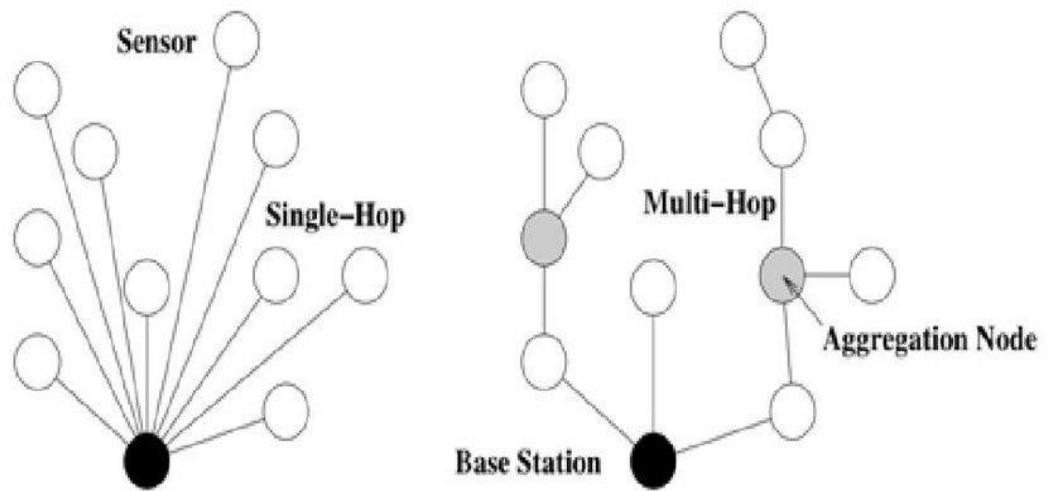


Figure 1.3: Single-hop and Multi-hop communication in VANET

A multi-hop link on a road for vehicular networks is effective and can be expanded to more than two vehicles for information exchange. As a result, the development of a connection for multi-hop connectivity between V2I and V2V on highways using a probabilistic approach reduces congestion. As a result, rather than building a multi-hop interconnection of lanes between the road of vehicles and the RSU, the functioning of helpful relay nodes is conceivable. VANET refers to networked queues and uses queue theory to assess multi-hop vehicular transmissions' end-to-end performance [23].

1.5. Examine the VANET network's performance

Furthermore, owing to the increased node mobilities, even single-hop inter-vehicle communication is unstable and suffers from severe channel fading and shadowing impacts. To be more explicit, we first create an analytical model to assess the system throughput of single-hop V2V transmissions, which takes into account channel fading and MAC contentions. Then we look at the linear vehicular network and characterize the vehicle as G/G/1 queues that are connected. End-to-end throughput and collective packet transmission time in the queuing system from sender to receiver are revealed by analyzing packet queuing time at each intermediate relay node. Finally, we use comprehensive simulations to back up our findings.

Network calculation could be used in VANETs to analyze network performance for assured QoS. It can be used to assess the effectiveness of network traffic performance. Long-term evaluation (LTE) capabilities for highway safety operations allow improved vehicle capacity with the shortest end-to-end delay. To support V2V broadcast, this can be done through centralized pathways. The IEEE 802.11p standard is used by the IVC systems for wireless connectivity in a vehicle network environment. Data exchange between high-speed vehicles as well as between vehicles and roadside infrastructure is necessary for this (RSU). A vehicle can be positioned inside the range of V2I and immediately connected to the range of RSU utilizing vehicular communications, according to a traditional VANET technique [24]. Network calculation, which has a rich and systematic structure, is used to examine the stochastic model. The E2E delay efficiency in VANET is investigated in this study. For the calculation of E2E latency, VANETs' LTE-based technologies are employed, which might lead to additional studies to boost the effectiveness of communication systems in the IVC system. The stochastic network calculus (SNC) is based on queuing networks, well-defined arrival times and service assurance.

1.6. VANET Security Attacks

The security of the VANET has become a serious concern in society. Before contacting the network's accessible services, all current stations need to be authenticated.

The assault includes an identifying process that exposes the entire network to severe effects. The authentication protections in a VANET system protect the safeguarded nodes from outside or within hackers who try to fool the network by employing a phony identity. Whenever a vehicle attempts to connect to the network or any service, the encrypting strategy process will take place. Attacks on privacy will be a fundamental security method in VANET communications, ensuring that only authorized users have access to data. In the absence of a mechanism, the VANET must preserve the confidentiality of transmitted messages, despite the fact that it is significantly more vulnerable to attacks. Attacks on availability play a critical part in the VANET, ensuring that the network is operational and providing necessary information at that time. Authentication and identification attacks have been a major topic of concern in VANET security [25]. Before they may connect to the available services, all of the real stations must be protected in the system. The attack uses an identifying mechanism that exposes the entire network to serious implications. The authenticating session will be conducted whenever a vehicle attempts to connect to the network or any service. Attacks on a vehicle's integrity and data trust must ensure that swapped data is not changed during transmission. These procedures help to protect information from being deleted, changed or supplemented. Non-repudiation attacks refer to the capacity to certify that the provider and acceptor are the only people who could really exchange messages. The non-abrogation of data source ensures that data is sent to the correct sender and the non-repudiation of introduction ensures that data is received only by authorized recipients.

Messages are regularly transmitted between vehicles in VANETs, as well as between vehicles and roadway infrastructural facilities [26] because many of these communications remain confidential, they must be protected for their integrity, validity, privacy, and secrecy. It is also important to consider the Real-time requirements of safety-related services as well as data consistency (the degree of reliability and applicability of the data of messages delivered by other automobiles). As previously stated, vehicles frequently share safety information via VANETs, and a vehicle takes vital judgments based on the information gathered from neighbours. Whether this information was wrong, unintended repercussions

may ensue, saving the lives of the vehicle's occupants in jeopardy. Users of the VANET may also be at risk from false information concerning traffic conditions, environmental hazards, and vehicle-related problems. In the event of a Sybil assault, when Sybil nodes create a false perception of traffic congestion for personal gain, a single-vehicle node might fake or manipulate traffic statistics. The key security issues in the context of automobiles at the physical, network, application, and physical layers are malicious nodes, DDoS attacks, authorization and confidentiality, SQL injections, intrusion prevention and control, hardware concerns, and cloud-based applications. The k-means technique is a good choice for this job due to its versatility in the extremely dynamic topology of VANETs. During the initial stage, a node clustering method is often required to spot a rogue node [27].

1.7. Management of mobility

The VANET's unique qualities pose issues and challenges for network control approaches, particularly vehicle mobility management methods that are critical for enabling reliable communication and ensuring user QoS requirements [28]. It offers a summary of VANET mobility management strategies. Mobility in VANETs is undeniably related to how drivers act and respond to barriers in a range and complex situations experienced at road infrastructure, at roadside BS on freeways, or inside a metropolitan centre. These limitations have a substantial impact on both the radio communication efficiency and the mobility paradigm. High mobility is one of the fundamental traits that distinguish vehicular networks from other types of wireless networks because vehicle speeds vary based on the environment. Although the movement of vehicles can be mostly predicted, one of the main issues with vehicular networks is how mobility affects connections and network topology. In contrast, a unit's ability to join or leave the connection quickly results in rapid topological changes. Researchers need to develop ways for controlling driving behaviour to address mobility issues. Because they can assess vehicle mobility models, vehicle operation, and traffic congestion, CNN and ANN are excellent AI algorithms. ANN can be used to predict mobility in Software-Defined Networking (SDN)-based vehicular networks, where the SDN controller is the component that builds mobility models based on the likelihood of user

movement models. The KNN algorithm can predict lane shifts and vehicle movement since it depends on each vehicle's accessibility to other cars with similar features.

While typical cellular mobility management solutions are quite established, the unique properties of VANET bring issues and obstacles [29] in terms of mobility management, as outlined in the following:

1.7.1. Frequent Handoff

The extremely mobile nature of vehicles in VANET necessitates regular handoff from source RSUs/RVs to destination RSUs/RVs. Handoff latency and packet loss during the handoff procedure can degrade the performance of the system and user QoS significantly. Creating handoff and pre-handoff strategies for specific vehicular applications in order to minimize the number of handoffs, handoff latency and packet loss rate are critical challenges that must be investigated [30].

1.7.2. Network Scenarios of Various Types

Because of the very dynamic nature of VANET, network separation can occur often, resulting in the impossibility of existing routes or the availability of better routes. Moreover, based on various application scenarios, the scope of VANET and the node density in the system may change dynamically. The task of designing adaptive handoff methods and protocols for dynamical network topologies and achieving optimal performance for varied application areas is a difficult one.

1.7.3. Choosing the Most Appropriate RSUs/RVs

In V2I and HV forms of communication, vehicles connect to external systems by accessing RSUs/RVs. Because a number of factors including the features of wireless links among vehicles and RSUs/RVs, the limited bandwidth of RSUs/RVs, the comparative shifting velocity of the RVs and source vehicles and others have a significant impact on user QoS and network performance. The best RSU/RV selection in VANET must be considered. To provide optimal handoff and accessing efficiency for users with various profiles and applications, the features of the source cars, RSUs/RVs, user apps and the external network must all be considered.

1.7.4. The Multiple Access Technology Integration

Various access methods such as Ad Hoc, cellular, WLAN and others are integrated into VANET to satisfy users' specifications. Vertical handoff between diverse access technologies and joint radio resource planning of many heterogeneous networks are two critical concerns that must be addressed.

1.7.5. Requirements for Different Applications

Safety-related products, for example are reactive to connectivity and packet delay yet some user applications, such as multi-media services need fast throughput and low delay jitter. It is a complex and challenging task to figure out how to improve handoff performance so that user QoS needs can be met for a variety of user applications.

1.7.6. Issues in QoS evaluation

Mobile vehicles carrying a variety of applications are expected to benefit from VANET's assured QoS [31]. Although certain QoS-related designs and approaches have been developed for VANET, ensuring user QoS during the user handoff process is a difficult challenge. Furthermore, for optimal resource usage and seamless handoff, it may be possible to combine both overall network allocation and user mobility management. QoS bargaining during handoff should be emphasized for certain user services, such as safety-related applications and user location management for better accessibility and timely delivery of services.

1.8. WSN and vehicular networks machine learning applications

Data-driven strategies are best for making decisions that are also appropriate for network dynamicity because of the enormous amount of data generated and gathered in the vehicular network. Machine learning is an effective technique for sustaining high performance in WSNs and VANETs while ensuring the robustness and dynamicity of massive amounts of data. Below is a list of a few ML applications in WSNs and VANETs [32].

1.8.1 Safety of the Network

Vehicular networks based upon deep neural networks utilizing unsupervised deep learning to set the parameters and work for the preprocessing stage are used in the intrusion detection system. The network can detect and classify anomalies with great precision using these types of techniques. It also predicts the next word that will be generated from each vehicle [33].

1.8.2. Predicting Vehicle Movement

Advanced driving assistance systems (ADAS) for inadvertent warning and collision avoidance benefit greatly from machine learning [34]. In networking protocols, it is crucial for handoff management, vehicle routing, and link scheduling. Furthermore, it has been found that using previously observed mobility patterns, probabilistic trajectory prediction based on variation GMM and Gaussian mixture models (GMM) can be useful in predicting the direction of the vehicle.

1.8.3. Accuracy

Estimation in the channel in today's wireless communications systems, determining accuracy is a time-consuming process. Due to quickly changing topology, brief channel contacts, and significant Doppler shifts, channel estimation is critical in vehicular networks. The time and frequency domain correlational time, multipath delay spreading, the nearby wireless environment and the vehicle speed position are all taken into account when determining wireless channel accuracy. Data gathered from various sources can be used to create an energy database that can be used to save the values of communication channels. A variety of machine learning technologies, like as deep learning and Bayesian learning, can be used to anticipate data, improve channel accuracy and provide more reliable channel estimation for current vehicular links.

1.8.4. Forecasting Traffic Flows

VANETs are used to store and manage quickly shifting traffic states and situations. Normal traffic data and information gathered from various automotive sensors are analyzed using machine learning (ML). Machine learning is useful for improving the flow and

anticipating traffic performance in order to provide a real-time response. During traffic prediction, a deep learning algorithm has been proposed. This method uses a rapidly changing traffic flow and a layered auto encoder to comprehend general features. Furthermore, training is carried out using a greedy layer-wise approach.

1.8.5. Load Balancing on WSN

Due to the frequency of data from the WSN, the network must deal with different patterns and transitions. In this case, learning-based techniques to load balancing in WSN could be an attractive option. The challenge of user organization with load balancing in an active environment has previously been developed online.

1.8.6. Location and Scheduling Routing

According to ML, estimated dynamics are a good option for networking protocol structures. The Hidden Markov model (HMM) is effective in predicting the position of the vehicle in the future based on past mobility data and mobility in VANET with V2I and V2V links [34].

1.8.7. Congestion Control

The main problem with WSNs and VANETs is congestion. As the network density increases, such as in congested and dense urban regions, this problem gets worse. Massive data collision happens when many cars try to use the same communication channels at once, which causes worse data packet loss and bottleneck conditions. The design of data congestion control systems benefits from the use of k-means clustering in ML [35].

1.8.8. Intelligent Wireless Management

The dilemma occurs as a result of the high signalling overhead and the difficulty in forming acceptable heterogeneous wireless and vehicular networks. Reinforcement learning is an efficient technique for maximizing a successful signalling ratio by connecting with the dynamic world in such situations.

1.8.9. Routing Techniques

The problem occurs as a result of the various approaches required for different routing reasons. VANETs are faced with a variety of unpredictable and fast-changing changes. Establishing a design or model that can be used in a variety of situations is still a challenging task. Despite extensive work to address various environment requirements for WSN and VANETs, a uniform approach to cater to routing needs is still lacking [36].

1.9. Using artificial intelligence to secure autonomous cars

In VANETs, Artificial Intelligence (AI) approaches for speech/image measurement and data transmission between V2V and V2I have been implemented. AI is overcoming the constraints and obstacles connected with VANETs [37]. Furthermore, the performance of pattern recognition methods related to ML determines the success of data-driven approaches. Vehicular ad hoc networks are the product of wireless communication technology advancements, intelligent transportation systems and automobile construction technology convergence. A VANET is a network of stationary (roadside units) and mobile (vehicles) entities that work together to exchange vital information on traffic patterns and other vehicles. The VANET has been the subject of study for more than ten years. In a similar vein, recent developments in computing technology have sped up the adoption of AI approaches across a variety of businesses (healthcare, medical, manufacturing, engineering, transport, and several others). Vehicular networks exchange data among vehicles, pedestrians, and infrastructure along the road in order to increase the efficiency and security of transportation systems. The techniques are: ML, DL, and SI. AI approaches are now being applied in a variety of real-world contexts due to their superior problem-solving abilities. Massive amounts of data as well as advancements in computationally efficient algorithms have contributed to the current success of AI systems.

An artificial intelligence system continuously learns from previous instances and relevant features in order to understand and recognize its environment [38]. It has the ability to think like a human and hence save lives, thereby improving pedestrian safety and automated driving. When deciding what actions are optimal for a specific scenario and its

final results, an individual is said to act intelligently. It can adapt to shifting aims and environments while also learning from the past. Agents can make decisions regarding the correct status of their locations and surroundings with the use of sensors that collect information about their surroundings. When communication is directed by beaconing in a VANET, a vehicle is oblivious of its current and forthcoming location, as well as the speed of other cars. The continuous transmission rate of the beacons is the only data provided to a vehicle. The sensor data fusion logic is a critical difficulty in realizing the assimilation of DSRC and GPS outcomes [39]. In a dynamic vehicular context, commonly utilized approaches such as Kalman and particle filters for a sub-optimum solution to Bayesian filter may struggle from collusive computational overhead, thus a localized method with pre-defined parameters to the posterior density is a good choice.

1.10. Techniques for Reducing Congestion

One of the most investigated areas in VANETs is congestion control. The channel is continuously watched, and the congestion control method is used whenever channel usage exceeds a predetermined threshold. To evaluate the impact of the algorithm, the channel is then discovered once more. Congestion control is based on three key parameters: transmit power management, data forwarding frequency and message scheduling in different channels based on priority [40]. To overcome the congestion problem in the past, a variety of optimization strategies were used. A meta-heuristic strategy for congestion control based on the Tabu search algorithm is one such method. Under variable traffic density, the suggested technique enhances performance in terms of packet loss and delay. In VANETs, the influence of decentralized congestion management on contention-based routing is discussed [41]. Also for periodic beacon transmission, the Decentralized Congestion Control (DCC) has been developed. It includes a thorough analysis of the classification of DCC methods for efficient V2V communication. A dynamic congestion control system monitors the control channel utilising adaptive congestion control, self-originated event-based recognition, and neighbour-originated event-based recognition (DCCS). The strategy

described above has been proven to enhance the overall performance of low latency, low packet loss and maximum throughput.

1.11. Routing Layer

Every network's performance evaluation is heavily influenced by routing. Because nodes enter and exit the network often, the quickest and least crowded path is used to convey the data over a number of hops. The topology is unknowable and dedicated pathways are not always accessible in VANETs. The network condition must be considered before forwarding data [42] because traditional routing techniques are incompatible with vehicular communication, the network's performance is hampered. That protocol should be able to perform localized operations in which routing decisions are only dependent on data present in the immediate vicinity. It removes the necessity for the node to be aware of the full network architecture, lowering control overhead [43]. The challenges of the routing layer include the following:

- a. Data management for routes
- b. Network segmentation
- c. Network density varies.

The following characteristics should be present in a perfect routing protocol for VANETs:

1. Exploration of the neighbourhood.
2. The capacity to forward data.
3. Information about the location.
4. Forecast where vehicles will be in the future.
5. Take into account the disparity in vehicle density.

1.12. VANET multi-layer challenges

The Physical (PHY) and MAC layer challenge presented by IEEE 1609.4 covers in depth the Channel Estimation at the PHY layer, the behaviour of Carrier Sense Multiple Access (CSMA) in large node densities, as well as various congestion control strategies and Multi-

Channel Operations. There has been a review of the effectiveness of single and multiple radios as well as some simulation results. The study also covered the development of the DSRC from the PHY and MAC Layer perspectives. It describes the problem using both single- and multiple-radio approaches and provides an overview of the WAVE Stack, Multi-Channel Communication, its challenges and solutions, as well as some unresolved concerns. The Self Organized Time Division Multiple Access (STDMA) has demonstrated success in VANETs in terms of scalability and reliability when compared to CSMA. There are numerous physical layer issues in VANETs:

1.12.1. Single and Dual Radio

It is still uncertain whether single and dual radio can coexist. Even while adding a second radio to a system of just one has several obvious advantages, it does not increase the effectiveness of safety awareness under the default system.

1.12.2. Propagation Model

Three different sorts of environments: rural, highway, and city: can use VANETs. The free space model, which is widely used for highways, is not very accurate because of environmental reflection. Open space cannot be utilized to mimic urbanization since there are many barriers in cities that cause shadowing and multipath fading.. Elements such as trees and hills can produce a lot of reflections in rural areas. As a result, the propagation model should take these factors into account.

1.12.3. Channel Selection

The Channel choosing at the Physical layer requires analytical and simulation research. The effectiveness of a game-theoretic strategy in choosing the appropriate channel and information rate is assessed.

1.12.4. Channel Estimation

In VANETs, advanced channel estimate algorithms are required to provide correct Channel State Information (CSI) [45].

1.12.5. Diversity Techniques

A variety of diversity tactics can be used to lessen the effects of fading and interference.

1.13. MAC protocol for VANET

The unique properties of VANETs necessitate careful quantitative and qualitative study, involved in developing MAC layer protocols. Figure 1.4 depicts the VANET's MAC protocol.

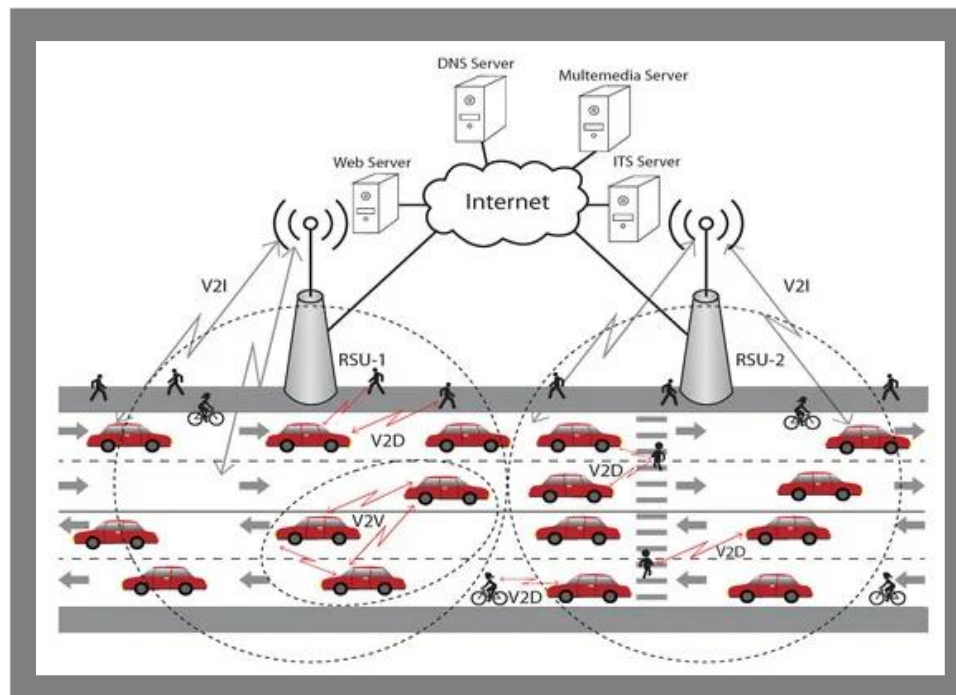


Figure 1.4: MAC protocol of VANET

Several servers are used on the internet, including Web, DNS, Multimedia and ITS servers. RSU is in charge of both V2D and V2V communications. When building MAC Protocol for VANETs, keep the following points in mind:

1.13.1. Bandwidth Restrictions

The Control Overhead in VANETs is increasing due to the frequent and quick changes in topology. When building a MAC Protocol for VANETs, keep bandwidth constraints in mind.

1.13.2. The MAC layer: An analytical study

Understanding the MAC Layer's nature is critical for designing an effective protocol that meets performance criteria. A significant amount of work has been put into stochastic modelling. Performance modelling and analysis are subject to the following conditions: internal/external accidents, node mobility, a range of access kinds, back-off counter freezing, saturated/unsaturated situations, and computational complexity. The propagation and collisions probabilities can be calculated with the use of Markov Chains. The simulation results and the mathematical regression model can be compared. A precise model will enable comprehension of MAC's behaviour. The IEEE 802.11p Enhanced Distributed Channel Access (EDCA) approach has so far been the subject of the majority of analytical modelling [46].

1.13.3. Contention Window (CW) dynamic adjustment

A node in a VANET should be able to identify congestion issues based on the order in which packets are received and alter the CW size in accordance with the number of consecutive packets received. In the literature, a number of Dynamical Correction of CW approaches have been developed, and superior receiving rates have been demonstrated through simulation. Congestion Control, a common strategy used in the CSMA/CA to prevent congestion, is closely related to this CW modification [47].

1.13.4. Congestion control

By modifying the Physical layer's characteristics and utilizing the MAC layer as a channel sensing mechanism, Decentralized Congestion Control (DCC) may be used as a cross-layer strategy. The congestion control systems offer high throughput. It is important to remember that a certain amount of frequency should be reserved for essential safety alerts, i.e., keeping channel congestion below a certain level. Algorithms for controlling congestion can be either proactive or reactive. However, research is currently being done on a third form of algorithm, called hybrid algorithms. Fairness, or the idea that the vehicles nearby each other should take share in reducing traffic, is the important component in creating

algorithms for congestion control. The major goals of the congestion control algorithms are the transmission power adjustment and the message rate adjustment [48].

1.13.5. Synchronization

Synchronization is placed centrally in VANETs. Currently, synchronization relies on Universal Time Coordination (UTC). In the event of a system-wide breakdown that could lead to the unreliability of the Global Clock, distributed synchronization solutions are necessary to coordinate in addition to centralized synchronization between nodes.

1.13.6. Efficient multi-channel utilization

IEEE 1609.4 first developed the Multi-Channel Operation. Two of the seven channels that are now available are the service channel (SCH) and the control channel. Safety messages are handled by the control channel, whereas non-safety applications are handled by the service channel. One service and one control channel comprise a synchronization interval (Sync Interval). To give continuous and alternative access, the channels change their operation. It is critical that the networks are used to promote the urgent signals in the most effective way possible. A strategy for making effective use of the SCH that allows service providers to disseminate their services to as many automobiles as feasible. The piece also draws attention to the potential for a concealed terminal condition in a building.

1.13.7. Scheduling vs. Containment

The use of Time Division Multiple Access rather than CSMA enhances performance, according to the studies referenced in the following section.

1.13.8. Exposed and Hidden Terminal Issues

Due to the IEEE 802.11p Control Channel's (CCH) broadcast nature, the Hidden and Exposed Node Dilemma can be one of the most difficult issues in VANETs [49].

1.14. VANET Applications

VANET applications are primarily divided into four groups:

- Public Safety application
- Non-Public Safety application
- Convenience application
- Productive application

The primary goal of public safety technology is to improve the overall safety of transportation systems. Real-time traffic conditions, post-crash alerts, traffic monitoring, collision mitigation and other safety applications are available. Non-public security application aims to improve driver comfort by offering value-added information such as nearby petrol stations, hotels, workshops and restrooms among other things. It is often advisable to use a public safety technology than a non-public safety technology. There are numerous applications that are used in many nations including Germany, Europe and Switzerland to make roads and automobiles safer. Convenience applications are mostly used to handle traffic congestion scenarios such as available parking spaces, route diversions and electronic toll collection among other things. New elements to the above-mentioned services that focus on converting traffic jam time into constructive work, such as reading the internet while awaiting in a vehicle for someone are known as productive activities. Additionally, when the average toll booth wait time is decreased to 1-2 minutes, fuel is saved [50].

1.15. Objectives

The objectives of the work are as follows:

- 1) To predict dynamic information about the vehicular environment using Artificial Intelligence.
- 2) To evaluate the impact of significant parameters on Vehicular communication.
- 3) To utilize the predicted information after validation for fast and reliable communication in vehicular networks.
- 4) To analyze the performance of a Machine learning-driven vehicular communication system.

1.16. Organization of the Thesis

This thesis comprises of following seven chapters:

Chapter 1 introduces VANET and its architecture, various VANET routing protocols, different types of security attacks, WSN and vehicular networks, machine learning applications, routing techniques, congestion reducing techniques and various VANET applications. Further, objectives of the proposed work have also been discussed here in this chapter.

Chapter 2 describes the study work's literature review. The current evaluation focuses on the performance of Routing Strategies of WSN as well as about Adhoc Networks

Chapter 3 describes the design and performance of Firefly Optimization algorithm additionally, Whale Optimization Algorithm WOA, in order to increase the performance characteristics such as Energy consumption, Drop, Throughput, Delay and Fairness Index (FI).

In chapter 4, using performance metrics, the result and explanation of the VANET system is discussed. This chapter compares the proposed equalization technique to existing VANET system equalization schemes.

Chapter 5 covers the background of SVM, HHO, DDoS attacks and security-based modified SVM.

In chapter 6, a hybrid metaheuristic based enhanced approach is discussed to achieve network stability which is based on ensemble approach with comparative performance.

Conclusion and future scope of the suggested study are discussed in chapter 7.

CHAPTER 2

LITERATURE SURVEY

2.1 Introduction

This section elaborates the analysis of related work based on VANETs in WSNetwork. Vehicular ad hoc network (VANET) has received a lot of attention recently because of its improved efficiency. Recent research has attempted to utilize the spatial degrees of freedom by incorporating various optimization techniques. Although the capacity performance may scale up as by various methods through analysis.

In this chapter, the topics discussed are as follows:

- ❖ Routing strategies
- ❖ Congestion control
- ❖ Packet forwarding
- ❖ Metaheuristic Approach

The various techniques involved in these topics are also discussed and their advantages & disadvantages are evaluated.

2.2. Routing strategies in WSNs

In 2020, G. S. Binu and B. Shajimohan [51] have proposed novel heuristic-based energy efficient routing strategy to maintain energy life time in WSNs. Using a novel African Buffalo-based two-tier data dissemination (AB-TTDD) technique to check the energy-drained node before the data transmission.

In 2018, Mohammad zakihasan, et.al.[52] have proposed a Cross-Layer Design of Quality of-Service (QoS) for WSNs to improve geographical quality.

In 2020, A. Sampathkumar, et.al.[53] have presented a method called lowworm swarm optimization for effectual load balancing and routing strategies in WNSs.

In 2019, Chuan Xu, et.al.[54] have suggested a Lifetime Maximization in WSN Energy-Efficient Region Source Routing Protocol (ER-SR).

In 2017, SarigaArjunan and Pothula Sujatha [55] have presented a Lifetime optimization of wireless sensor networks employing a hybrid algorithm based on ACO and fuzzy based imbalanced clustering.

In 2020, Deyu Lin [56] proposed Compressive Sensing and an Energy-Saving Routing Integrated Economic Theory to Extend the Lifespan of WSNs.

In 2020, M.L.M. Peixoto, et.al.[57] have suggested A fog computing-based traffic data clustering system for VANETs.

In 2019, Quan Wang, et.al.[58] have presented Compressive Sensing-Based Clustering Routing Protocol for WSNs with Low Energy Consumption.

In 2019, Matteo michelette, et.al.[59] have suggested a method of Combining Cluster Head Election (CER-CH) and Routing in Heterogeneous WSNs.

In 2019, G. S. S. Chalapath, et.al.[60] have presented an Efficient and Simple Time Synchronization (E-SATS) Protocol for Cluster-based Wireless Sensor Networks.

In 2018, Anwar Khan, et.al. [61] have proposed Taxonomy, Research Challenges, Routing Strategies, and Future Directions for Underwater Wireless Sensor Network Routing Protocols.

In 2015, Tarachand Amgoth and Prasanta K. Jana [62] have presented an energy-conscious routing approach for wireless sensor networks has been devised.

In 2018, AfraaAttiah, et.al.[63] have suggested An Evolutionary Routing Game for Wireless Sensor Networks by Energy Balancing.

In 2015, Zhezhuang Xu, et.al. [64] have presented Balancing Energy Consumption in Wireless Sensor Networks Using a Hybrid Clustering and Routing Strategy.

In 2015, Mohammad Hossein Anisi, et.al.[65] have proposed Energy harvesting and battery-powered routing are employed in wireless sensor networks.

In 2017, Boyuan Sun and Donghui Li [66] have presented A Multi-Attribute Trust-Aware Routing Protocol for Wireless Sensor Networks.

In 2019, Yu He, et.al. [67] have proposed to safeguard the anonymity of the source location, WSNs for the Internet of Things employ a sector-based random routing mechanism.

In 2017, Wenlong Chen, et.al. [68] have suggested to secure source anonymity in WSNs, a restricted random routing mechanism is used.

In 2020, K. Thangaramya, et.al. [69] have presented an intelligent fuzzy rule-based method with outlier detection is employed for safe routing in WSN.

In 2015, Bing Zeng and Yan Dong [70] have presented an upgraded harmony search-based routing method for wireless sensor networks that uses less energy.

2.3. Congestion control strategies in VANETs

In 2018, Nouredine Haouari, et.al. [71] have proposed Density-aware Congestion Control in VANETs with the Application in Reliability Analysis. SLDE, a density estimation strategy for VANETs.

In 2018, Feng Lyu, et.al.[72] have suggested Link Perception in VANETs to manage distributed beacon congestion.

In 2020, Mamata Rath, et.al.[73] have presented Improved VANET Traffic Control System Using Mobile Agents.

In 2020, Nikita Lyamin, et.al.[74] have suggested VANETs featuring Age-of-Information-Aware Decentralized Congestion Control. System (C-ITS).

In 2020, Anirudh Paranjothi, et.al.[75] have suggested employing network tomography to construct a congestion detection and control method for connected vehicles.

In E.A. Feukeu and T. Zuva [76] have suggested VANET Storm Mitigation Utilizing Dynamic Broadcast. The Dynamic Broadcast Storm Mitigation Algorithm (DBSMA) is a tool that can be used to address the broadcast storm issue in a vehicular network (VN).

In 2017, Kashif Naseer Quresh, et.al.[77] have suggested safety applications in automotive ad hoc networks, a dynamic congestion control scheme has been developed.

In 2018, ForoughGoudarzi and Hamid Asgari [78] have proposed a method of Controlling the power of non-cooperative beacons in VANETs.

In 2019, Ata ullah, et.al.[79] have proposed Emergency Message Dissemination Schemes Based on Congestion VANET and Vehicular FoG Computing Avoidance in emergency message broadcasting strategies relies on congestion avoidance scenarios.

In 2018, Jamal Toutouh and EnriqueAlba [80] have proposed Swarm-based traffic sharing in vehicular networks.

In 2021, Banoth Ravi and JaisinghThangaraj [81] have suggested multi-hop cooperative data dissemination in VANETs using stochastic traffic flow modelling.

In 2018, Nikita Lyamin, et.al.[82] have presented Malicious Network Traffic Detection in VANETs Using Artificial Intelligence.

In 2021, Arun Kumar Sangaiah, et.al.[83] have suggested Linear Adaptive Congestion Control with Data Dissemination Model Optimization in Vehicle-to-Vehicle Communication.

In 2019, Sahil Garg,et.al.[84] have presented Security Framework for Big Data Analytics in VANETs based on Edge Computing. A smart security framework for VANETs outfitted with edge computing nodes and 5G technology has been designed to enhance the capabilities of communication and computation in the modern smart city environment.

In 2021, R. C. Karpagalakshmi, et.al.[85] have proposed An Effective Traffic Management System for Congestion Reduction in High-Density Areas the Connected Dominating Set Forwarding (CDSF) Framework in VANETs.

In 2015, Nasrin Taherkhani and Samuel Pierre [86] have Utilizing a Machine Learning Clustering Algorithm, a Centralized and Localized Data Congestion Control Strategy for Vehicular Ad Hoc Networks was developed.

In 2015, Nasrin Taherkhani and Samuel Pierre [87] have presented Improving dynamic and distributed congestion control in car ad hoc networks.

In 2017, Hayder M. Amer, et.al. [88] have suggested A Game Theory Approach to Congestion Control in Vehicular Ad Hoc Networks.

In 2015, Arrate Alonso¹ and Christoph F. Mecklenbrauker [89] have presented Decentralized Congestion Control Reliability with Varying VANET Density.

In 2017, Chen Chen, et.al. [90] have presented A bargaining game method to information congestion reduction in the Internet of Vehicles.

2.4. Congestion control based on parameters

In 2018, Sofiane Zemouri, et.al. [91] have suggested Strict Beaconing Requirements in Urban VANETs.

In 2019, Wenfeng Li, et.al.[92] have presented A Reliable Congestion Control Mechanism for Safety Applications in Urban VANETs.

In 2019, Xiaofeng Liu and ArunitaJaekel [93] have briefly presented the Problems, Analysis, and Solutions of V2V Safety Communication Congestion.

In 2020, Sayed Jobaer, et.al.[94] have proposed A UAV-Assisted Hybrid Scheme for Urban Road Safety Based on VANETs.

In 2020, Byeong-moon cho, et.al.[95] have suggested a Congestion Control in Vehicular Cyber-Physical Systems with Channel Awareness.

In 2019, R. Regin and T. Menakadevi [96] have presented a Dynamic Clustering Mechanism Based on Node Density to Avoid Congestion Control in Vehicular Ad Hoc Networks.

In 2018, Hendrik-Jorn G unther, et.al. [97] have proposed the Effects of Decentralized Congestion Control on Collective Perception in Dense Traffic Scenarios.

In 2020, Gurpreet Singh Shahi, et.al.[98] have presented an Adaptive Mechanism for Congestion Control in Smart Vehicular Network Multimetric road guidance mechanism (MRGM), which analyses traffic congestion circumstances using several metrics and suggests effective best routes to cars depending on those conditions.

In 2020, Meng Wang, et.al.[99] have suggested Adaptive beacon message transmission power is being examined in VANETs.

In 2020, Parag Sewalkar and Jochen Seitz [100] have presented Congestion Control for Vehicle-to-Pedestrian Communication Using Multi-Channel Clustering.

2.4.1. Adhoc Network

In 2020, R. Regin¹ & T. Menakadevi [101] have presented A unique clustering technique for preventing congestion in car ad-hoc networks has been devised, which uses node density as a function of received signal intensity.

In 2020, Roniel S. de Sousa, et.al.[102] have suggested A distributed and low-overhead traffic congestion management system for car ad hoc networks. DisTraC is a vehicle ad hoc network protocol.

In 2020, Hayder Amer et.al.[103] have presented Non-Cooperative Game-Based Congestion Control for Data Rate Optimization in Vehicular Ad Hoc Networks.

In 2020, HamidehFatemidokht and MarjanKuchaki Rafsanjani [104] have proposed An Efficient Clustering Algorithm Based on QoS and Monitoring of Malicious Vehicles in Vehicular Ad Hoc Networks.

In 2019, Lakshmanaprabu S.K, et.al.[105] have suggested ant colony optimization-based routing in vehicular ad hoc networks as a result of big data technologies.

In 2018, Weidong Zhang, et.al.[106] have proposed A Distributed Infrastructure-Free Traffic Optimization System Based on Vehicular Ad Hoc Networks for Urban Environments.

In 2019, Jiashuai Wang, et.al. [107] have presented A Hop-By-Hop Bidirectional Congestion Control Algorithm for Ad-Hoc Networks Based on Contention.

In 2016, Varun Kumar Sharma and Mahesh Kumar [108] have suggested an adaptive congestion control approach is utilized in mobile ad-hoc networks.

In 2016, M. Rajesh and J. M. Gnanasekar [109] have offered wireless ad-hoc network congestion control using the adhoc protocol scheme.

In 2017, M.Rajesh, et.al. [110] have presented self-adjust hybrid model congestion control scheme for heterogeneous wireless ad hoc networks.

In 2020, FarkhanaMughtar, et.al.[111] have proposed Named Data Networking Congestion Control for Wireless Ad Hoc Networks.

In 2019, Hannan Bin Liaqat, et.al. [112] have gives about Current Status and Future Directions in Socially-Aware Congestion Control in Ad-Hoc Networks.

In 2020, Jogendra Kumar, et.al. [113] have presented Mobile ad hoc networks employ congestion control, load balancing, and adaptive routing algorithms for the random waypoint model.

In 2017, M. S. Gowtham and Kamalraj Subramaniam [114] have suggested Congestion control and packet recovery are employed in a MANET using a cross-layer technique.

In 2020, Juan Pablo Astudillo Leon, et.al. [115] have presented A Fair and Distributed Congestion Control Mechanism for Smart Grid Neighbourhood Area Networks.

Moreover, table 2.1 shows both the parameters of the congestion control of VANETs and adhoc and author name, findings, methods and parameters are plotted inside the table 2.1.

Table 2.1:Parameters of the congestion control of VANETs and Adhoc

S.NO.	Author /year	Findings	Methods used	Parameters
1	ForoughGoudarzi, et.al. (2017) [116]	Controlling the Non-Cooperative Beacon Rate and Awareness for VANETs	Control of the non-cooperative beacon rate and awareness (NORAC)	Beacon rate and CBR is constant
2	SoufieneDjahel and YacineGhamri-Doudane. (2012) [117]	A Strong Congestion Control Scheme for Rapid and Reliable Safety Message Dissemination in VANETs	Intelligent Transportation Systems (ITS)	Beacon delivery ratio is 20%
3	Miguel Sepulcre, et.al. (2010) [118]	VANETs' Communication Channel: Application-Based Congestion Control Policy	Cooperative Awareness Messages (CAMs)	Packet transmission rate is 40%
4	Sebastian Kuhlorgen, et.al. (2019) [119]	Evaluation of Multi-hop Packet Prioritization for Decentralized	priority queuing (PQ)	CBR f=0.634.

		Congestion Control in VANETs		
5	Jagruti Sahoo, et.al. (2013) [120]	Congestion-Controlled-Coordinator-Based MAC for	congestion-controlled-coordinator-based MAC (CCC-MAC)	Delivering beacons to around 98%
6	Mohamed Salah Bouassida and M. Shawky (2009) [121]	Formal Verification and Performance Evaluation of a Cooperative Congestion Control Approach in VANETs	Cooperative and fully distributed congestion control	Service Packets-Loss Rate vs Mean Number of Neighbors (mean message size = 500 bytes, and message generation rate = 150 msgs/s)
7	Fei Ye, et.al. (2010) [122]	Congestion Control to Achieve Optimal Broadcast Efficiency in VANETs	Contention control algorithm	Performance about 95%
8	Mohammad Reza Jabbarpour, et.al. (2019) [123]	A cross-layer congestion control concept is employed in urban traffic situations.	Dedicated Short Range Communications (DSRC)	Decrease the packet traffic congestion

9	Tessa Tielert, et.al. (2020) [124]	Rate Adaptation Based Congestion Control for Vehicle Safety Communications: Design Methodology and Evaluation	Oriented protocol named PULSAR.	Piggybacking efficiency at 0.6 CBR
10	Andrea Vesco, et.al. (2020) [125]	Investigating the Effectiveness of Decentralized Congestion Control in Vehicular Networks	Decentralized Congestion Control (DCC) mechanisms	Load varies from 24% to 72% and packet size grows from 100 to 600 bytes
11	Omar Chakroun and SoumayaCherkaoui (2014) [126]	For 802.11p VANETs, overhead-free congestion control and data distribution	Multi-hop routing and access channel techniques	Improve the packet reception rate (PRR) and reduce the End-to-End (E2E)
12	BengiAygün, et.al. (2016) [127]	Congestion control for vehicular communications that is aware of the environment and context in terms of both power and rate	Decentralized Congestion Control (DCC) algorithms	ECPR can improve the average message rate by 18%

2.5. Routing protocols and its technical issues in VANET

In 2019, Ankita Srivastava, et.al. [128] have suggested the issues and current solutions in VANET location-based routing protocols.

In 2018, Predictive Geographic Routing Protocol for VANET has been presented by Ramin Karimi and Saeed Shokrollahi [129]. a Predictive Spatial Routing Model. This problem is solved by the protocol PGRP, which improves connectivity.

In 2018, Kamlesh Kumar Rana, et.al. [130] have proposed Improved Directional Location Added Routing Protocol Analytical Analysis for VANETS

In 2018, Saifullah Cho, et.al. [131] have presented A novel forwarding mechanism based on geographical information moves packets from source to destination node, and a traffic information for route selection enables for computing the Expected Connectivity Degree (ECD) on various segments.

In 2018, TawfiqNebbou, et.al. [132] have suggested slightly backwards routing protocol for VANET.

In 2018,HoseinBagherlou and Ali Ghaffari [133] have proposed Using the simulated annealing method and neural networks, we develop a routing system for automobile ad hoc networks.

In 2020, Ravie ChandrenMuniyandi, et.al [135] have proposed A VANET location-assisted routing protocol with genetic optimization based on rectangular position estimation.

In 2021, Raghu Ramamoorthy and MenakadeviThangavelu [136] have presented an enhanced hybrid ant colony optimization routing algorithm has been developed for automotive adhoc networks.

In 2019, Christy Jackson Joshua¹ and Vijayakumar Varadarajan [137] have suggested A multi objective firefly algorithm approach to routing protocols in VANETs as an optimization framework.

In 2017, Ramesh C. Poonia [138] have analyzed Swarm intelligence is used to assess the effectiveness of vehicle ad hoc network routing systems.

In 2020, K. Satheshkumar and S. Mangai [139] have suggested Message distribution that is both energy efficient and quick for vehicle ad hoc networks, there is a routing protocol.

In 2019, Shahab Haider, et.al. [140] have proposed A Robust Routing Protocol for the Dissemination of Warning Messages in VANETs.

In 2018, VANETs QoS-based routing protocols for ITS infotainment services based on multi-constrained capabilities have been described by Michael Oche et al. [141].

In 2019, leticialemusc`rdenas, et.al. [142] have proposed A Probability-Based Multimetric Routing Protocol for Vehicular Ad Hoc Networks in Urban Scenarios.

In 2019, Omar Sami Oubbati, among others UAV-assisted supporting services connection in urban VANETs has been proposed by [144].

In 2019, Sabri Allani, et.al. [145] have plotted a method Towards a Smarter Directional Data Aggregation in VANETs. Smart Directional Data Aggregation is a revolutionary data aggregation methodology (SDDA).

In 2017, Ahmad Abuashour and Michel Kadoch [146] have presented The Cluster-Based Routing Protocol's performance in the VANET has been enhanced.

In 2019, Suman Malik and Prasant Kumar Sahu [147] have posted a comparison of routing protocols for VANETs was conducted.

In 2020,Ravie ChandrenMuniyandi, et.al. [148] have suggested A Genetically Optimized Location Aided Routing Protocol for VANET based on Rectangular Estimation of Position.

In 2015,Ram Shringer Raw, et.al. [149] have proposed the Analysis of the Directional-Location Aided Routing Protocol in VANETs.

In 2017, Daxin Tian, et.al. [150] have shown that aVANET Routing Protocol Influenced by Microbes.

In 2018, Irshad Ahmed Abbasi, et.al. [151] have presented Routing Protocol for VANETs in City Environments Based on Dynamic Multiple Junction Selection.

In 2021, Prashant Kumar Shrivastava and L.K. Vishwamitra [152] have proposed A comparison of proactive and reactive routing systems was carried out in the VANET environment.

In 2017, J.M. García-Campos, et.al. [153] have suggested A Methodology for Evaluating Routing Protocols in VANETs Using Reliable Simulations.

In 2018, Omar Sami Oubbati, among others UAV-assisted supporting services connection in urban VANETs has been proposed by [144].

In 2016, Using tabu search, Elham Moridi and Hamid Barati [155] have developed a practical multi-level routing system for the VANET.

In 2017, A method of load balancing in an EMHR-energy-based hybrid routing protocol with mobility concerns, interference-aware bandwidth estimation is used. for VANET-WSN communication has been presented by Linda F. Mohaisen and Laurie L. Joiner [156].

2.6. Packet forwarding approaches by machine learning algorithms

In 2021,Hind Bangui, et.al. [157] have proposed Invasion detection in VANET using a mixed machine learning model.

In 2021, JothyNadarajan and Jayanthi Kaliyaperumal [158] have presented Machine intelligence, applied in the future generation to construct a QOS aware and secure routing algorithm in VANET.

In 2020, Jinqiaowu, et.al. [159] have suggested RSU-Assisted Traffic-Aware Routing for Urban VANETs Utilizing Reinforcement Learning. RSU-assisted Q-learning-based Traffic-Aware Routing is a route optimization technology for urban VANETs (QTAR).

In this 2019, Yujie Tang, et.al. [160] have presented Heterogeneous VANET Delay-Minimization Routing with Machine Learning-Based Mobility Prediction.

In 2019, Xuefeng Ji, et.al. [161] have proposed a method to maintain the forwarding path in VANET as fresh as feasible, Reinforcement Learning is employed. Reinforcement learning is a type of learning that is based on positive reinforcement-based Hybrid Routing Algorithm (RHR) that can track traffic in real time packet-carry-on and the possible pathways with their status information as a source of real-time feedback for routing. RHR continues to exist.

In 2018, Degan Zhang, et.al. [162] have suggested VANET implementation of a novel self-adaptive routing service algorithm. The dependability of a link is assessed and employed as a critical parameter in the development of a new routing system.

In 2020, Xian Guo, et.al. [163] have proposed A Bayesian Receiver-Forwarding Decision Scheme for NDN-VANET. A Bayesian-based Receiver Forwarding Decision (BRFD) mechanism is employed in the NDN-VANET to lessen the broadcast storm issue brought on by interest packets.

In 2018, Fan Li, et.al. [164] have presented a Reinforcement Learning for Hierarchical Routing in Vehicular Ad Hoc Networks. QGrid is a reinforcement learning-based hierarchical system that improves message delivery ratio with the least amount of delay and hops achievable.

In 2021, Kumar Sharshembiev, et.al. [165] have suggested A method for identifying protocol noncompliance in car Ad Hoc networks based on machine learning classification.

In 2020, Kun Yu, et.al. [166] have presented Network Routing Based on Machine Learning. The basic paradigm of network routing based on machine learning.

In 2021, Namit Gupta, et.al. [167] have presented FPGA hardware and machine learning were used to analyze the performance of the DSDV and OLSR wireless sensor network routing algorithms.

In 2021, Jyoti Grover, et.al. [168] have suggested Multiple Misbehavior Detection in VANET Using Machine Learning.

In 2016, Celimuge Wu, et.al. [169] have presented A Data Storage Scheme for Vehicular Ad Hoc Networks Based on Reinforcement Learning.

In 2013, Ahmed Soua and Hossam Afifi. [170] have suggested VANET adaptive data gathering protocol based on reinforcement learning.

In 2013, Celimuge et.al. [171] have proposed A Flexible, Portable and Practical Fuzzy Constraint Q-Learning Approach to Routing in VANETs.

In 2015, Celimuge Wu, et.al. [172] have suggested Fuzzy Logic and RL-Based Parameter Adaptation for Packet Size-Aware Broadcasting in VANETs.

In 2016, Yuliya Shilova, et.al. [173] have proposed A Reinforcement Learning Approach to Network Routing Using Full Echo Q-Routing with Adaptive Learning Rates.

In 2019, Mojtaba Mohammadnezhad and Ali Ghaffari [174] have suggested A hybrid routing method based on an imperialist competitive algorithm and RBF neural networks for VANETs is being developed.

In 2020, Ankur Nahar and Debasis Das [175] have presented Adaptive Reinforcement is a type of reinforcement that adapts to the situation. Software Defined Vehicular Network Routing.

2.7. Analysis of meta-heuristics optimization based malicious activity detection in VANETs

In 2018, A Multi cluster head dolphin swarm optimized IDS for VANET based on hybrid fuzzy multi-criteria decision making has been proposed by Sparsh Sharma and Ajay Kaul [176].

In 2018, A Security Aware Fuzzy Enhanced Reliable Ant Colony Optimization Routing in Vehicular Ad hoc Networks has been reported by Hang Zhang et al. [177]. A fuzzy logic

module is used by the SAFERACO routing protocol to recognize and exclude problematic nodes from the routing process.

In 2018, K. DeepaThilak and A. Amuthan [178] have proposed DDoS mitigation on VANETs utilizing an enhanced Ant Colony-based Optimization Algorithm based on cellular automata.

In 2020, S. Prabakeran and T. Sethukarasi [179] have suggested the hybrid chaotic particle dragonfly swarm technique is the best solution for detecting and preventing rogue nodes in VANETs. DDoS attack detection and prevention on VANETs using a fast and secure HCPDS-based system.

In 2020, Kuldeep Narayan Tripathi, et.al. [180] have proposed A New Reputation-Based Algorithm (RBA) to Detect Malicious Nodes in Vehicular Ad Hoc Networks (VANETs).

In 2021, HamidehFatemidokht, et.al. [181] have proposed an Efficient and Secure Routing Protocol for Vehicular Ad Hoc Networks in Intelligent Transportation Systems Based on Artificial Intelligence Algorithms with UAV-Assisted.

In 2020, NeeluKhare, et.al. [182] have suggested Intrusion Detection using Spider Monkey Optimization and a Deep Neural Network Hybrid Classifier Model.

In 2020, A solution for VANET routing attack prevention utilizing an artificial swarm algorithm has been proposed by Vasiliy Krundyshev, et al. [183]. Particle Swarm Optimization (PSO) is a particle swarm optimization method used in the NDN-VANET.

In 2019, Ayoub Alsarhan, et.al. [184] have presented Intrusion Detection in Smart Vehicular Networks with Machine Learning-Driven Optimization. Road safety has been significantly improved by vehicular ad hoc networks (VANETs).

In 2020, Chaker Abdelaziz Kerrache, et.al. [185] have suggested A Technique for Detecting Malicious and Selfish Nodes in VANETs Using UAVs. A trust paradigm aided by unmanned aerial vehicles (UAVs) is presented.

In 2020, Kuldeep Narayan Tripathi, et.al. [186] have proposed a method for Detecting Packet Dropping Attacks in Vehicular Ad Hoc Networks with the Entity.

In 2020, A. Balamurugan, et.al. [187] have presented dependable emergency data sharing in VANETs under NLOS conditions; a raccoon optimization algorithm-based precise placement technique is used.

In 2020, a Trust-Based Clustering Mechanism for IoT-Enabled Vehicular Ad-Hoc Networks that is Stable and Centralized has been described by Kamran Ahmadawan, et al. [188]. overcoming these difficulties through elements of trust.

In 2016, Omar Abdel Wahab, et.al. [189] have suggested an SVM-based intelligent detection model is employed for clustering vehicular ad hoc networks.

In 2018, Tao Zhang and Quanyan Zhu [190] have proposed Collaborative Intrusion Detection Systems for VANETs with Distributed Privacy Protection.

In 2018, Amr Tolba, et.al. [191] have presented Collision Attack Avoidance in VANETs Using a Trust-Based Distributed Authentication Method.

In 2020, FatemehsadatMirsadeghi, et. al. [192] suggested that a trust-based authentication approach for clustered vehicular ad hoc networks is needed to generate dependable and stable clusters that contribute to the stability of the whole network. For this reason, [193] estimates the trust degree of each vehicle by combining the trust between cars and the trust between the vehicle and Road Side Units (RSUs), and Cluster Heads (CHs) are selected based on this estimated trust degree.

In 2018, Chunhua Zhang, et.al. [194] have proposed a misbehaviour detection system based on an SVM and the Dempster-Shafer theory of evidence to fend off attacks using misleading messages and message suppression.

In 2021, Nitha C Velayudhan, et.al. [195] have proposed An Efficient EPORP Technique for Sybil Attack in Urban VANETs with RSU Detection and Location Privacy.

In 2020, Nisha Malik, et.al. [196] have presented a secure message exchange through block chain technology, solutions for security and trust management for vehicle networks.

In 2021, Zhixia Zhang, et.al. [197] have suggested An Intelligent Intrusion Detection Algorithm Based on Many-Objective Optimization for Improving Vehicular Network Security in 6G.

In 2020, Zihao Zhu, et.al. [198] have presented a reputation-based cooperative content delivery using parked automobiles in vehicular ad-hoc networks.

In 2018, S. Baskar and V. R. Sarma Dhulipala [199] have suggested for vehicular ad hoc networks, a trusted node and quality of service-based energy multi path routing protocol has been developed.

In 2021, BechirAlaya and Lamaasellami [200] have planned a Securing urban VANET networks using a clustering approach and symmetric/asymmetric cryptography scheme.

In 2020, RaenuKolandaishamy, et.al. [201] have preferred a stream position performance analysis model for cluster-based routing in VANET based on DDoS attack detection.

In 2019, Junwei Liang et al. [202] have designed a filter model based on hidden generalised mixture transition distribution model networks for intrusion detection in vehicle ad hoc.

In 2021, Sudha Anbalagan, et.al. [203] have proposed RSU Placement Mechanism for Software Defined-IoV based on Machine Learning that is both efficient and safe.

In 2021, Junwei Liang, et.al. [204] have planned An Efficient and Collaborative Framework for IDSs in Vehicular Networks Using a Markov-Based Reputation Scheme.

Moreover, table 2.2 shows the analysis of optimization based malicious activity detection in VANETs and author name, findings, purpose of the research and results achieved are plotted inside the table.

Table 2.2: Analysis of optimization based malicious activity detection in VANETs

S.NO	Author/Year	Algorithm used	Purpose of the research	Parameters evaluated	Results achieved
1	Fuad A. Ghaleb, et.al.2020 [205], TarakNandy, et.al.2020 [206], Erfan A. Shams, et.al.2017 [207], M. Poongodi, et.al.2019 [207], Saurabh Dey, et.al.2019 [208].	Machine learning	Intrusion detection in VANET	Accuracy, F-measure, latency	Latency reduced
2	Pradeep Sadashiv Khot and Udaykumar Naik.2021.[209], Mahmoud Hashem Eiza, et.al.2015.[210], Mahmoud Moadeli and Wim Vanderbauwhede 2010. [211], Kubilay Demir, et.al.2016.[212].	QoS-aware routing algorithm	QOS aware and secured routing.	accuracy, sensitivity, average delay, packet delivery ratio.	Has more robustness with the high intensity
3	Jun Tao, et.al.2014.[213], Adi makma, et.al.2016. [214], AbirMchergui, et.al. 2020.[215], Jaya	Q-learning-based Traffic-Aware Routing (QTAR)	RSU-Assisted Traffic-Aware Routing	packet delivery ratio. Average end-to-end delay.	Reduce the possibility of packet loss

	SubalakshmiRamamoorthi, et.al.2019.[216], Farooque Hassan Kumbhar, et.al.2020.[217]				
4	Chengyue Lu, et.al.2021.[218], Long Luo, et.al.2021.[219], ClaysonCeles, et.al.2020.[220], Saleh a. Alghamd. 2021.[221].	Machine learning	Delay- Minimizatio n Routing for Heterogeneo us VANETs	Mobility model, packet loss	Mobility is accurate
5	Mohammad Al-Rabayah and Robert Malaney.2012. [221], Salim Bitam, et.al.2013.[222], MarwaneAyaida, et.al.2013.[223], Di Wu, et.al.2013.[224].	Hybrid Routing algorithm (RHR)	Keep Forwarding Path Freshest in VANET	Network scale, request frequency and vehicle velocity	route and lookup-route, which uses the improved low- costQ- Learning algorithm
6	Sunitha Safavat and Danda B. Rawat. 2015.[225], ArnauRovira-Sugranes. 2010.[226], Fatima Zohra Bousbaa, et.al.2020.[227],	An Ant Colony Optimization (ACO) algorithm	Intelligent Transportati on Systems Artificial Intelligence Algorithms for	packet delivery ratio, end- to-end delay, and number of hops	This package by 16 percent for delivery and 7 percent for detection

	N. Gomathi1 · Mukund B. Wagh.2018. [228].		Vehicular Ad Hoc Networks with UAV Support		
7	Jitendra Kumar Samriya, and Narander Kumar. 2020.[229], Seok-Jun Bu, et.al.2022.[230], J. Sathya Priya, et.al.2021.[231], Scaria Alexa and T Dhiliphan Rajkumar.2021. [232].	spider monkey optimization (SMO) algorithm	Hybrid Classifier Model for Intrusion Detection	Accuracy, F-measure, and Precision.	92% accuracy, 99.5% and 92.7% of precision, 99.5% and 92.8% of recall and 99.6% and 92.7% of F1-score
8	M. O. Kalinin, et.al.2018.[233], Abhishek Kumar and Dr. Neetesh Gupta.2020. [234], Samuel Kofi Erskine and Khaled M. Elleithy.2019. [235], Zhongshan Zhang, et.al.2013. [236].	Artificial swarm algorithm	VANET protection against routing attacks	Throughput, packet delivery ratio	Throughput increased by 20%, the share of delivered packets by 30%, and the delay time decreased by 40%.
9	Sang-Woong Lee, et.al.2021.[237],	Machine Learning-	Intrusion Detection in	Malicious node's	Dropping some packets.

	Mohammad Tayyab, et.al.2020.[238], Asmaa a. Elsaedy, et.al.2020. [239], Muhammad Zeeshan Asghar, et.al.2019. [240].	driven Optimization	Smart Vehicular Networks	arrival rates	
10	Nadia Haddadou, et.al.2015. [241], Khattab M Ali Alheeti, et.al.2015.[242], Kuldeep Narayan Tripathi and S. C. Sharma. 2018.[243].	Adaptive detection threshold	Detection of Malicious and Selfish Nodes in VANETs	Detection threshold adaptive control, Detection ratio	Packet ratio is maximum
11	Sarah Oubabas, et.al. 2018.[244], N. SreeDivya, et.al.2021.[245], Xuanxia Yao, et.al.2016.[246], Farhan Ahmad, et.al.2018.[247]	ECT Algorithm: Entity- Centric Combined Trust	Attack Packet Dropping in Vehicle Ad Hoc Networks Detected (VANETs)	data delivery fraction and end-to-end delay	Packet dropping destrained.
12	Rana Rageh Shaaban, et.al. 2017.[248], Christopher Chembe.	Raccoon optimization algorithm	a precise location method for trustworthy	Rate of awareness, localization error.	16.21%, 14.38%, and 15.16% for dissemination

	2016.[249], Shimaa A. Abdel Hakeem, et.al.2022.[250].		emergency data distribution in VANETs		rate, positioning accuracy, and vehicle awareness, respectively.
13	Kamran ahmadawan, et.al.2020.[251], Khalid Haseeb, et.al.2020.[252], Kamran ahmadawan, et.al.2019.[253], Khalid Haseeb, et.al.2019.[254].	StabTrust clustering algorithm	A Stable and Centralized Trust-Based Clustering Mechanism for IoT Enabled Vehicular Ad-Hoc Networks	Energy consumption	End-to-end packet delivery lets the network use less energy, which helps the StabTrust get closer to being a green VANET.

CHAPTER – 3

MALICIOUS ACTIVITY DETECTION BASED ON DYNAMIC VANET

3.1 Introduction

In recent times, road safety issues are increasing day by day that makes the researchers to provide solution for that because road accidents are one of the main reasons for the mortality of people. According to the WHO, traffic accidents are currently the eighth biggest cause of death, but by 2030 they may move up to the fifth place. Therefore, to overcome the traffic issues including accidents, risk of hindrance, stopping problem and financial overhead, VANET (Vehicular Ad-hoc Networks) is the effective solution due to its capability like it permits the vehicle to interact with each other.

3.1.1 VANET (Vehicular Ad-hoc Networks)

VANET is a unique subcategory of the MANETs, which require each vehicle to deliver messages to every vehicle by utilizing RSU (Road side units) or multi-hop communication. In converse to MANET, VANETs are the self-organized and dynamic mobile networks, which are constructed based on the movable vehicles and road communication amenities.

- **Applications of VANET**

Generally, it is utilized in numerous circumstances such as transmitting the messages in emergency situation, safeness of vehicle, mobile entertainment. Additionally, various safety and non-safety assistances are offered by it for the road user via V2V (vehicle-to-vehicle) and V2I (vehicle-to-infrastructure) connections using OBU (on board unit) and RSU (road side unit) devices. In road traffics, VANETS are utilized as a component to improve the road safety by allotting the drivers about any mischances occurred there or providing web access to the traveller. Normally, GPS and Sensors are mostly utilized in vehicle to monitor the status of the vehicle for instance performance of the device, geographic representation of vehicle position and the road conditions. Even though, there is some difficulties in VANET like development in topology and repeated separation of links. Therefore, the enhancement of VANET's reliability becomes difficult task because data are transferred via multi-hop wireless network. So that, routing protocols are employed in VANET.

- **Routing Protocols**

There are several routing protocols in VANET that are reactive, proactive, hybrid and geographic based protocols and based on topology, position, geocast, broadcast, and cluster, these protocols. From these routing protocols, the cluster-based routing protocol is performed efficiently because it requires less energy among the sensor nodes. Whereas, the cluster-based routing protocol (hybrid routing protocol) amalgamates the features of the reactive and the proactive routing protocols and these protocols come under the topology-based routing protocols.

Furthermore, Cluster can be defined as nodes of the hybrid network and these are combined in a certain portion. Cluster based protocols are constructed to maximize the scalability of the network through permitting the nodes to interact with the clusters by selected cluster heads through the proactive routing protocol. If the interaction happens among the clusters the reactive routing protocols are activated.

Furthermore, the effectiveness of the protocol is expressed through the QoS (Quality of service) parameters that are latency, delay, packet delivery ratio, throughput, etc. Whereas QoS objectives are attained through the proactive and reactive protocols because it has a capability to select the alternate routes in advance and even in a link failure it can lessen the time required for convergence. QoS parameters may reduce the performance of the routing protocol therefore optimization is essential to tune the constants and parameters of the timers that maximize the effectiveness of protocol in terms of accuracy so that hybrid optimization algorithms are incorporated with the cluster-based routing protocol because optimization provides the capability to routing protocols for resolving the multi-objective issues and enhancing the computation speed of the protocol.

3.2 Hybrid Meta-Heuristic Algorithm

The proposed model based on a hybrid meta-heuristic algorithm to identify malicious activities in the dynamic environment of VANET is the major subject of this section. The development of a hybrid model is based on Firefly Optimization and Whale Optimization algorithm that the combination is named Hybrid Firefly with Whale Optimization Algorithm

(HFWOA). The proposed model enables a highly effective communication paradigm that mainly supports for optimizing the communication between the clusters in the network and help to fetch the cluster head by means of considering the parameters including the distance, distrust value, velocity, and proportional bandwidth. These parameters support to deal with the limitation of mobility of vehicle based on QoS parameters. The QoS parameters are highly required for the selection of cluster head for managing the loads by means of executing the proper distribution strategy towards the entire network. In addition, the vehicular network connectivity and stability can be ensured through this protocol. In this model, cluster head selection process is initially executed for selecting or electing the trustier vehicle as Cluster Head. In this process, the entire vehicles are participated to elect the cluster head simultaneously. Then based on the cluster head the neighbouring nodes are selecting as the gateways to transmit the packet and forming the clusters. At last, in case failure in gateways the immediate alternative solution to found for effective transaction through the proposed model is achieved.

The suggested VANET-based concept includes an integrated Global Positioning System (GPS) that allows the entire fleet of cars to retrieve the network's geographic data. The HFWOA-VANET Model is associated with Firefly Optimization technique and Whale Optimization technique. The following section describes about each technique in detail.

3.3. Background Model

3.3.1 Firefly Optimization Algorithm

The firefly optimization algorithm is developed based on the activity of Firefly's flashing characteristics. Its flashing characteristics can be categorized by three rules such as

- The main characteristics of Firefly is unisex nature; therefore, the fireflies attract other fireflies not only for their sex;
- The second characteristic is its brightness, which supports for attraction process. Therefore, a firefly with less brightness depends on brighter firefly or less bright firefly follows brighter. Moreover, a distance of their journey is significant due to if

distance increases subsequently brightness decreases. In case none of the firefly's brightness is better than a specific firefly, a random moving process will take place.

- The third point is that the landscape of the objective function that has to be adjusted affects or analyses the objective function that is dependent on the brightness of a firefly

The variable i represents the degree of brightness, r_{ij} indicates the distance between each firefly, and j denotes its attractiveness.

$$I(r) = \frac{I_s}{r^2} \quad (3.1)$$

As earlier discussed, the firefly's brightness is depending on objective function. The objective function is required to reveal the recent position of its objective function $f(x)$.

$$I_i = f(x_i) \quad (3.2)$$

As discussed earlier, the firefly brightness helps to attract the other firefly in which a brighter firefly is always attracted by lesser firefly because of its certain attractiveness value β based on their distances.

$$\beta(r) = \beta_0 e^{-\gamma r^2} \quad (3.3)$$

Where, the β_0 represents the Attractiveness value of firefly at $r=0$ and the γ represents the Media light absorption coefficient.

- **Movement towards attractive firefly**

The firefly movement towards the brighter firefly can mathematically represented by

$$X_{i+1} = X_i + \beta_0 e^{-\gamma r^2} (X_j - X_i) + \alpha \left(rand - \frac{1}{2} \right) \quad (3.4)$$

Here i is the movement of a firefly at X_i position move forward towards a brighter firefly at X_j , X_i represents the position of lower brightness firefly, X_j represents the position of brighter firefly and the j is representing the brighter firefly.

Where, the condition $\beta_0 e^{-\gamma r^2} ij (X_j - X_i)$ is because of attraction process of the firefly X_j ; therefore, if $\beta_0=0$ it formed to be a simple random movement. The firefly attractiveness is compared with prior position. Then the firefly position is updated by means of higher attractiveness value. Otherwise, the firefly will be relying on its already existed position. At last, the condition termination process is executed by its predefined iterations.

In the next section, the description about another optimization algorithm (WOA) to support with Firefly Optimization algorithm is mentioned.

3.3.2. Whale Optimization algorithm (WOA)

The humpback whales' hunting behaviour is taken into account when developing the "Whale optimization algorithm." This type of whale's usual preys is Krill's and a small school of fish by means of executing the bubble-net feeding strategy. In this process, the whale goes 12 m downwards to execute spiral or nine shaped bubbles for making confusion to their preys. Then, they move upward to reach sea surface for hunting prey. In hunting process, at least two whales are involving for encircling and bubble nets strategy. The systematic procedures are given below to get more details (Figure 3.1)

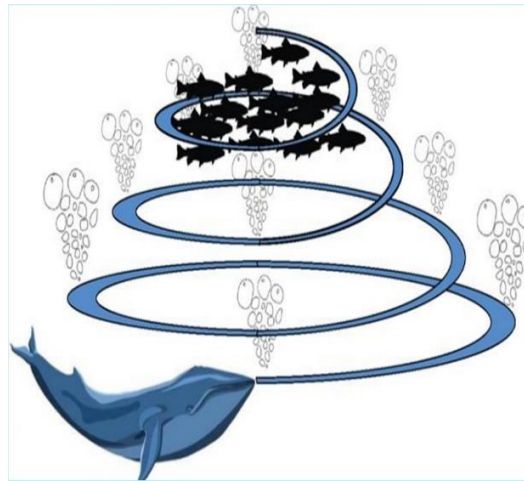


Figure. 3.1 Bubble-net feeding behaviour in humpback whales

- **Encircling prey equation**

Since WOA first assumes that its prey is the goal, a humpback whale may observe the location of its prey and encircle it. The ideal search agent is taken into consideration after examining the greatest available option. Similarly, additional search agents can alter their positions in order to outperform one another by increasing the maximum iteration. The mathematical structure of this operation is shown in the following equation.

$$D = |C \cdot X^*(t) - X(t)| \quad (3.5)$$

$$X(t + 1) = X^*(t) - A \cdot D \quad (3.6)$$

Where, the t is representing the current iteration, A and C represent the Coefficient Vectors, X^* is so far, obtained best solution's position vector and X is the Position Vector.

In this process, X^* is periodically updated in every iteration process based on determining the best solution.

$$A = 2a \cdot r - a \quad (3.7)$$

$$C = 2 \cdot r \quad (3.8)$$

In exploration and exploitation processes, a range of variable is decreased from 2 to 0. The exploitation process executes global search process to fetch optimized solution. Meanwhile, the exploitation takes local search by executing big jumps to the search space. Therefore, unnecessary steps can be ignored and get results effectively. Where, the r is random number that has a range from 0,1.

- **Bubble-net attacking Strategy**

A significant step of Whale attacking process is bubble-net strategy which can be pointed out by two processes such as shrinking encircling and spiral updating. In Fig 3.2 (a) and Fig 3.2 (b), the bubble-net attacking strategies are drawn clearly. The following provides the description about processes.

- **Shrinking encircling mechanism**

The “A” can be considered as a significant variable that will decrease linearly from 2 to 0th range in the course of iteration. This process shows big difference in “A” at the interval [-1,1]. The new position of the search agents may be in the same area as their previous position. In Fig. 3, the possible positions from X and Y to X^* and Y^* are accomplished on the interval [-1,1] as the foundation for the condition $0 \leq A \leq 1$ in a 2D space.

- **Spiral updating position**

The spiral updating strategy can be constructed by analyzing the distance of whale and the prey are required to calculate. Then the spiral path is determined based on the position of both the whales and its preys in order to execute the movement in terms of helix-shaped by whales. This process is determined by the following equation below.

$$X(t + 1) = D' \cdot e^{bl} \cdot \cos(2\pi l) + X^*(t) \quad (3.9)$$

Where, the D' is distance of whale $X(t)$ towards prey $X^*(t)$, the t is iteration, The l is a random number in the range [-1, 1], and the b indicates the shape of a logarithmic spiral.

$$X(t + 1) = \begin{cases} X^*(t) - A \cdot D & \text{if } p < 0.5 \\ D' \cdot e^{bl} \cdot \cos(2\pi l) + X^*(t) & \text{if } p > 0.5 \end{cases} \quad (3.10)$$

In this process, there is a 50% chance that the spiral model or the shrinking encircling mechanism will be used to update the position of the whale.

- **Search for prey**

The humpback whales also execute the random searching process to find prey which differs from the exploitation phase. This process is achieved by determining the variation of the vector. If the condition $|A| < 1$, the exploitation condition is taken place by executing the updating position to the current best individual. Conversely, if $|A| > 1$ comes the exploration process is executing the random selection process to choose individual for the global optimum. Moreover, based on this procedure updating the position is executed, which is mathematically denoted below.

$$D = |C \cdot X_{rand} - X| \quad (3.11)$$

$$X(t + 1) = X_{rand} - A \cdot D \quad (3.12)$$

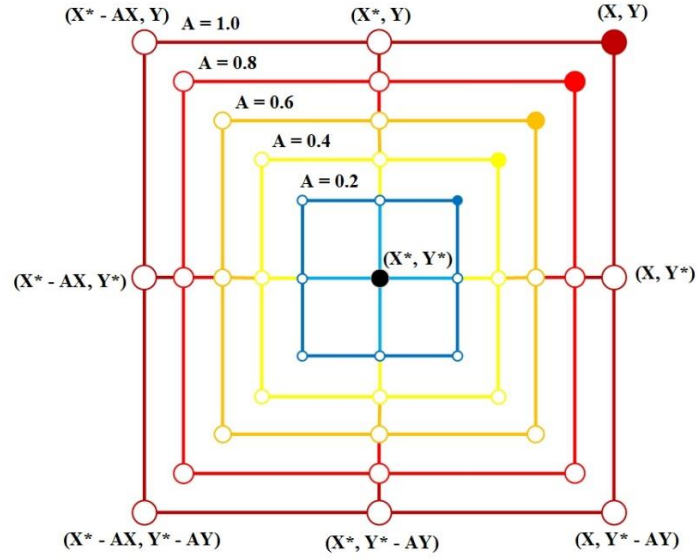


Figure 3.2 (a) Shrinking encircling mechanism

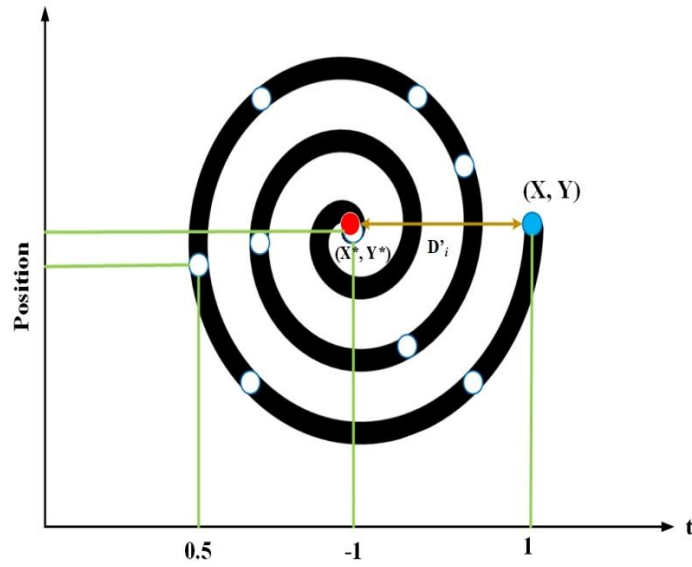


Figure 3.2 (b) Spiral updating position mechanism

Fig.3.2 WOA has a bubble-net search mechanism in place (X^* is the best result so far)

3.4. Intelligent Clustering via HFWOA

In VANET environment, a complex network structure and a traffic density led to a more complicated network structure. Therefore, an effective clustering technique is required to mitigate the complexity of the network by enhancing the network stability through minimizing number of clusters. In minimum clustering environment, a less amount of Cluster Head for enhancing the communication performance by adopting the HFWOA-VANET in a complex environment. The cluster-head selection process is required for obtaining an effective communication by means of transferring information between each node or cluster member. Therefore, a hybrid meta-heuristic algorithm is developed by the combination of two algorithms such as Firefly optimization and Whale Optimization Algorithm. Thus, the combination of algorithm is HFWOA to provide a solution set of effective CH in VANETs environment. In HFWOA-VANET framework, each search agent denotes a solution set has QoS values including distance, distrust value, and proportional bandwidth. The QoS parameters are considered for optimizing the Cluster Head selection process by ensuring the loads of vehicle in the network that are properly distributed. Thus, the network protocol can ensure the vehicular network stability and connectivity. The cluster head can take responsibly to form cluster, data gathering among the cluster area, the transaction between CH to other CHs, distribute the load evenly, maintain network stability and at last cluster termination process. In this clustering approach, the CHs has a direct contact with the Base Station (BS). As far as a cluster-head selection process is significant, a neighbourhood (gateway) selection is also an important process to retransmit the data and forming a respective cluster.

Moreover, each vehicle has a data space to manage the neighbourhood details where all the vehicles' data are initially stored as normal. Then, the malicious node can be diagnosed by HFWOA algorithm and separated it to malicious data space. The neighbourhood data helps to execute better communication in clusters that prevents from information loss. As discussed, all vehicles are managing the neighbourhood list based on beacon messages generated by each vehicle with QoS value. The QoS value is incorporated with the vehicle id, position of the vehicle, distrust value, and speed. In fact, the neighbourhood list with

QoS value of vehicles also illustrates about the availability of number of neighbour's vehicles in a network area. Moreover, the network stability can be managed by analyzing the velocity and distance of the vehicles. These parameters help to determine the CH and CM with significant distance and velocity to data transfer. This process helps to prolong the lifetime of the network and mitigate the network communication failure.

The following formulas are considering for determining the velocity and distance of the vehicle. The formula of velocity ration, average speed, velocity, Distance Ratio, and residual distance are shown in equ (3.13), equ (3.14) and equ (3.15), respectively.

$$\text{Vel_rat} = \text{Vel_C}/\text{Avg_Sp}; \quad (3.13)$$

$$\text{Res_Dist} = \text{M_Dis}-\text{CP}; \quad (3.14)$$

$$\text{D_rat} = \text{Res_Dist}/\text{M_Dis} \quad (3.15)$$

Where, CP denotes the Vehicles' current position, M_Dis denotes the Distance calculation between source and target, the Vel_rat denotes the Velocity Ratio, the Avg_Sp denotes the Average Speed, the Vel_C is representing the Velocity, the D_rat denotes the Distance Ration, and the Res_Dist denotes the ratio of residual distance towards destination.

The other considerable QoS parameter is distrust value that helps to distinguish the behaviour of vehicle while transferring hello messages between vehicles to vehicles. This value is essential for vehicle to join in a new network where Upon joining a network, a vehicle's initial mistrust value is 1 that is $V_d=1$, the same value is assigned to all vehicles in a group. The entire vehicles distrust value is also stored in neighbourhood table. Where, the V_d represents the distrust value of vehicle.

Furthermore, as discussed above, the QoS value is highly significant to calculate the performance of the vehicle using the neighbourhood table for analyzing the vehicle's information. The following provides the formula of analyzing QoS value.

$$\text{QoS}_v = (\text{Ban}_v \times \text{Nei}_v \times \frac{\text{D_rat}}{\text{Vel_C}}) / V_d \quad (3.16)$$

Where, the QoS_v represents the Vehicle's QoS value, the Ban_v denotes the Available bandwidth, the Nei_v denotes the Number of neighbours, v is representing the Vehicle.

The proposed HFWOA algorithm helps to analyze the QoS value of vehicle and the vehicle that has maximum QoS value will become a Cluster Head. This procedure is repeated until all of the vehicles in the cluster have been updated, and HFWOA can be used to differentiate between the present clusters when new vehicles join or existing vehicles leave.

Each vehicle is initially added to the white list, and if its distrust rating rises above a certain level, it is moved to the malevolent list. This step ensures the importance of a threshold value for determining and separating malicious node. The following equation shows the condition of the threshold value

$$\delta = e^{\varphi} \quad 0 \leq \varphi \leq K_v - 1 \quad (3.17)$$

Where, the K_v denotes the average number of vehicles, the N_{avg} represents average number of vehicles, the T_{avg} denotes the typical transmission range

$$K_v = T_{avg}/N_{avg} \quad (3.18)$$

By analyzing these conditions, the abnormal behaviour of the vehicle can determine. In addition, in this model the vehicles in a cluster act as verifier which analyze the misbehaviour by means of threshold value and distrust values. In case, a vehicle QoS value especially distrust value is determined as larger than the threshold value it is considered as malicious and it directly moved to the malicious vehicle list from normal vehicle list. The following flowchart shows that how the HFWOA algorithm analyze the QoS value to differentiate the malicious vehicle from normal vehicle.

The flowchart of proposed model in Fig 3.3 is shown below:

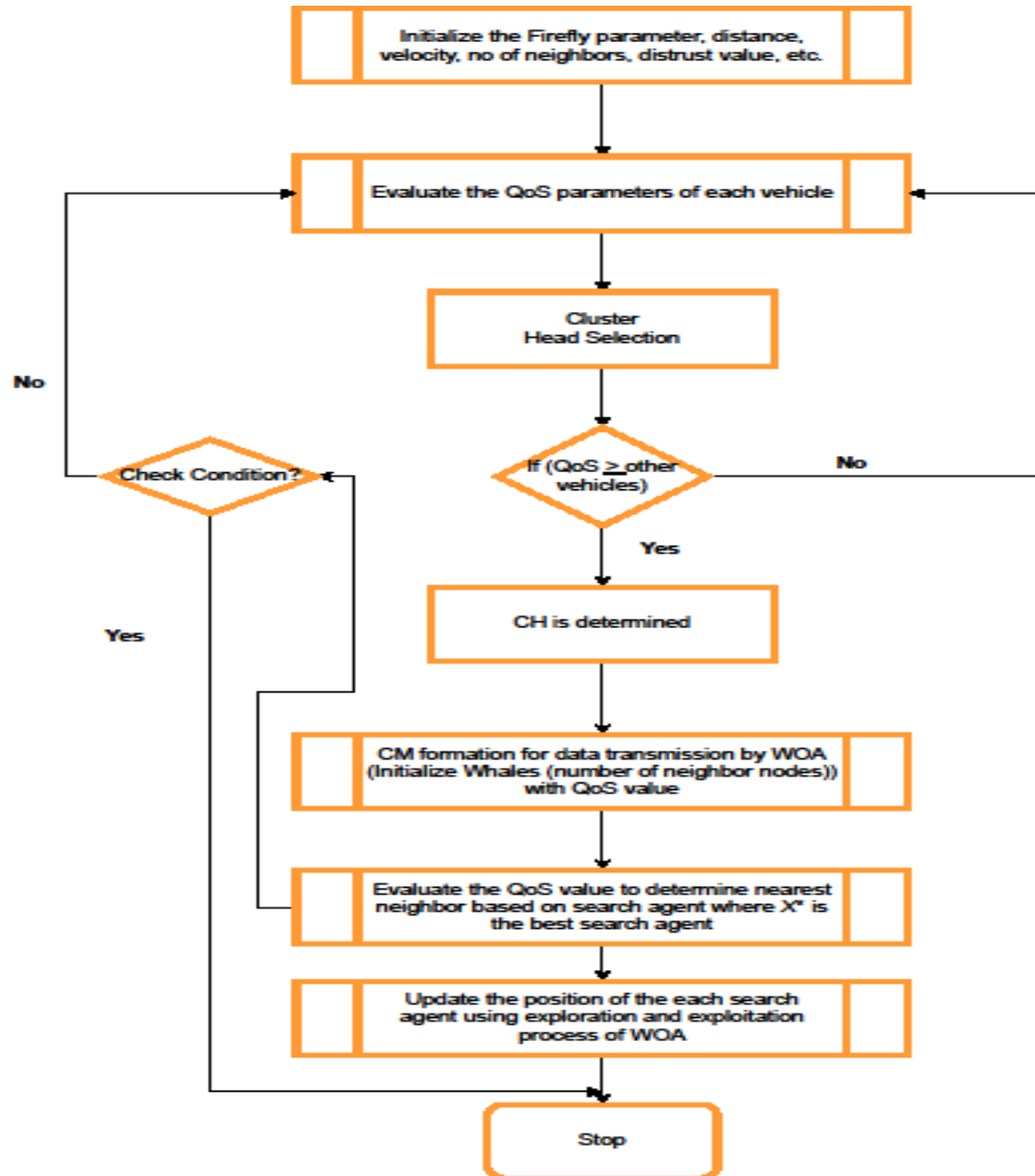


Figure 3.3.Flowchart of the HFWOA-VANET

The next section provides the detailed information about the results obtained through the proposed model. Similarly, a comparative analysis also incorporated in the following section to prove the HFWOA-VANET is highly effective.

3.5. Results and Discussions

Discussion of the results of the implementation process is covered in this section. Energy usage, Drop, Throughput, Delay, and Fairness Index are the five metrics used to determine the output of this implementation method (FI). Furthermore, each parameter is plotted as a graph-based on Node and speed. The whole implementation process is performed on the network simulator named NS2. Furthermore, the proposed HFWOA-Vanet is compared with the existing QMM-Vanet. The graphs attained based on node and speed are demonstrated and discussed in the following sections.

- *Node*

In this section we are discussing the results which are obtained from the implementation process based on Node. Here, five nodes are considered for each parameter and they are 20, 30, 40, 50, and 60. The obtained energy consumption Vs Node values are plotted as a Table 3.1 and graph in figure 3.4.

Table 3.1: Node values Vs Energy consumption

Node	Energy Consumption(Joules)	
	HFWOA-Vanet	QMM-Vanet[118]
20	98	99
30	98	99
40	97	98
50	97	98
60	97	98

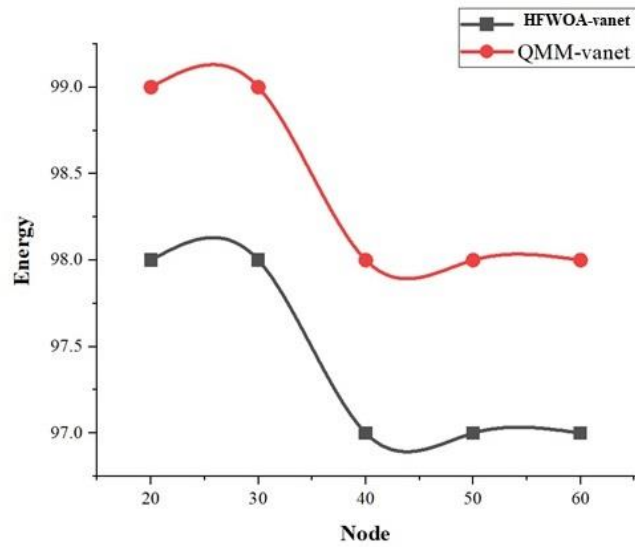


Figure 3.4. Graphical representation for Energy consumption Vs Node

The above table 3.1 and diagram (figure 3.4) are demonstrating the graphical representation of Energy consumption Vs Node for the proposed HFWOA-Vanet and existing QMM-Vanet. Here, the proposed HFWOA-Vanet is reducing from 98 to 97 for considered nodes. This value is lower than the existing QMM-Vanet value that reducing from 99 to 98. Likewise, the table 3.2 and figure 3.5 are illustrating the graphical representation of Drop Vs Node.

Table 3. 2: Node Vs Drop

Node	Drop(%)	
	HFWOA-Vanet	QMM-Vanet[118]
20	0.984475	0.996241
30	0.986718	0.996136
40	0.97245	0.995207
50	0.978949	0.994582
60	0.974986	0.993653

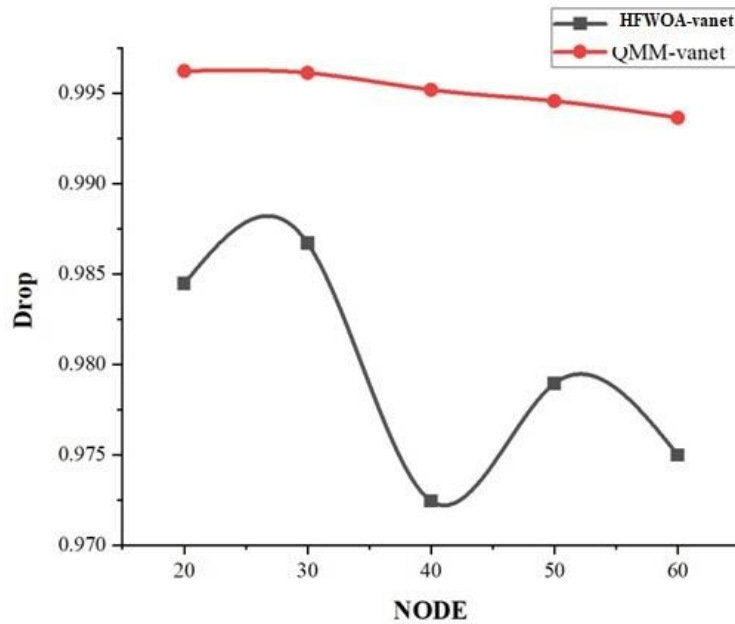


Figure 3.5.Graphical representation for Drop Vs Node

From the above Table 3.2 and diagram (in figure 3.5), the existing QMM-Vanet is reduced from 0.996 to 0.993. On other hand, the proposed HFWOA-Vanet is attained 0.984 at 20 Node and it is decreased to 0.972 at 40th Node after that reached 0.974 drop at 60th Node which is lower than the existing QMM-Vanet. Similarly, the table 3.3 and figure 3.6 are demonstrating the graphical representation for the Throughput Vs Node.

Table 3. 3:Node Vs Throughput

Node	Throughput(Kbps)	
	HFWOA-Vanet	QMM-Vanet[118]
20	20196	19349
30	20763	19334
40	23402	19165
50	22308	18921
60	21097	17100

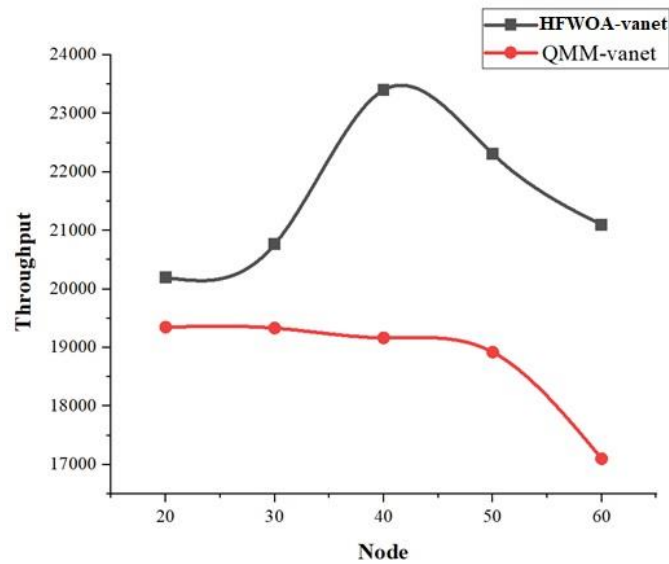


Figure 3.6.Graphical representation for Throughput Vs Node

The above table 3.3 and diagram (figure 3.6) shows the variations of Throughput for HFWOA-Vanet and QMM-Vanet. Here, the existing QMM-Vanet is reducing from 19349 to 17100 throughput. Nevertheless, the proposed HFWOA-Vanet is attaining 20196 at 20th Node and increased to 23402 at 40th Node after that it reached 21097. The proposed technique's throughput is higher than the existing technique. Likewise, the table 3.4 and figure 3.7 are demonstrating the graphical representation for Delay Vs Node.

Table 3.4: Node Vs Delay

Node	Delay(s)	
	HFWOA-Vanet	QMM-Vanet[118]
20	0.422682	0.553047
30	0.584858	1.059783
40	0.845636	0.961704
50	0.810469	1.228869
60	0.963607	1.683063

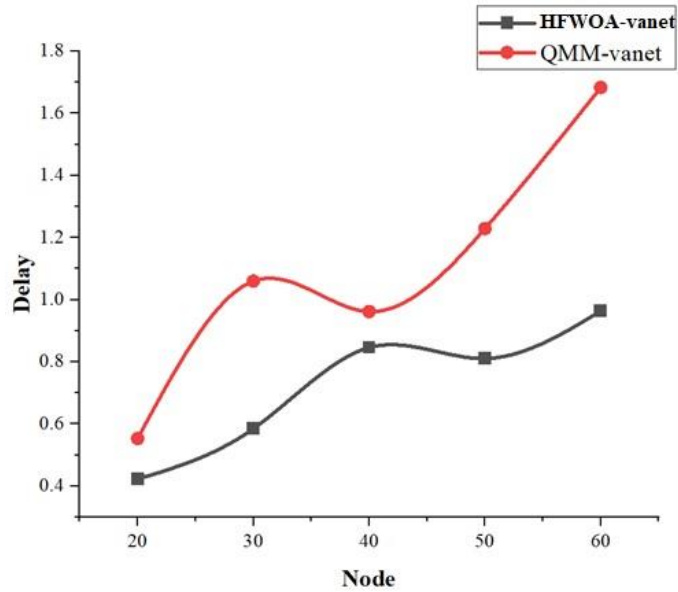


Figure 3.7.Graphical representation for Delay Vs Node

The delay time of the existing QMM-Vanet is increased from 0.55 to 1.68 sec. Still, the proposed HFWOA-Vanet is slightly increased from 0.422 to 0.96 sec which is lower than the existing QMM-Vanet. Moreover, the table 3.5 and figure 3.8 are denoting the graphical representation of Fairness Index (FI) Vs Node.

Table 3.5:Node Vs Fairness Index

Node	Fairness Index	
	HFWOA-Vanet	QMM-Vanet[118]
20	6	3.8698
30	4	2.577867
40	3	2.4915
50	2	1.90784
60	2	1.482

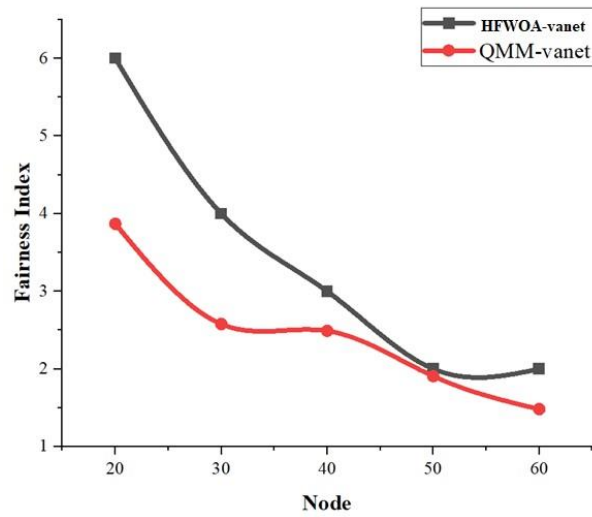


Figure 3.8.Graphical representation for Fairness index (FI) Vs Node

The fairness index for the existing QMM-Vanet is decreased from 3.86 to 1.48. But the proposed HFWOA-Vanet is decreased from 6 to 2 which is higher than the existing technique. The following section is demonstrating the obtained results for the considered parameters Vs Speed.

- **Speed**

This section is demonstrating the outcomes which are obtained from the execution process, based on Speed. Here, also five-speed variations such as 20, 40, 60, 80, and 100 are

considered. The table 3.6 and figure 3.9 demonstrating the graphical representation for energy consumption Vs speed.

Table 3. 6:Speed Vs Energy consumption

Speed	Energy Consumption(Joules)	
	HFWOA-Vanet	QMM-Vanet[118]
20	1940	1980
40	3880	3960
60	5820	5940
80	7760	7920
100	9700	9900

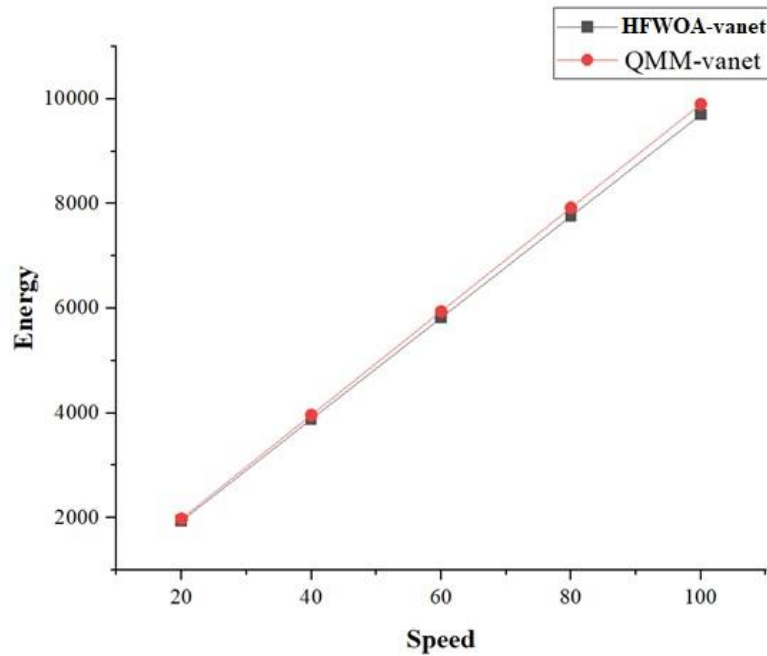


Figure 3.9.Graphical representation for Energy consumption Vs Speed

The energy consumption of the existing QMM-Vanet based on Speed is increased from 1980 to 9900. On other hand, the proposed HFWOA-Vanet is increased from 1940 to 9700, which is slightly lower than the existing technique. Similarly, the table 3.7 and figure 3.10 are demonstrating the graphical representations for Drop Vs Speed values.

Table 3. 7:*Speed values Vs Drop Values*

Speed	Drop(%)	
	HFWOA-Vanet	QMM-Vanet[118]
20	19.493056	19.873056
40	38.999454	39.746111
60	58.499181	59.619167
80	77.998908	79.492222
100	97.498635	99.3652786

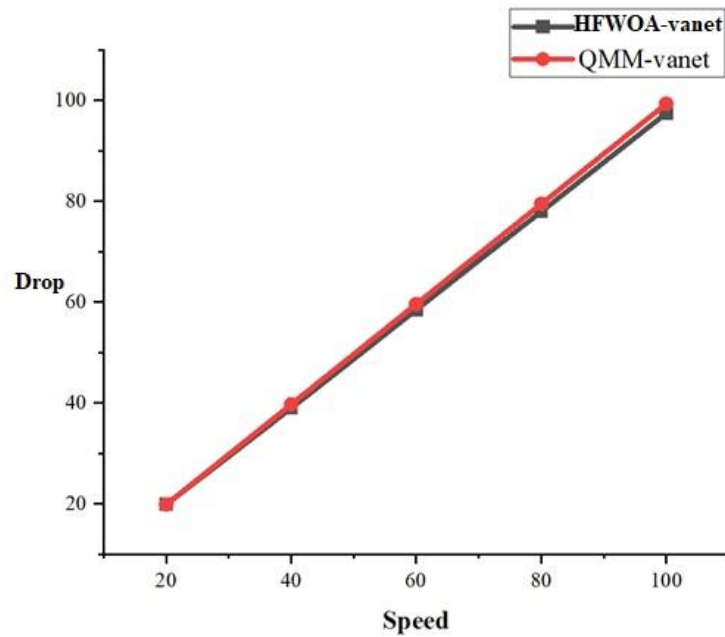


Figure 3.10. *Graphical representation for Drop Vs Speed*

In the Drop Vs Speed graph (figure 3.10), the existing QMM-VANET is increased from 19.87 to 99.36. Nevertheless, the proposed HFWOA-VANET is increased from 19.49 to 97.49, which is slightly lower than the existing technique. Likewise, the table 3.8 and figure 3.11 are demonstrating the graphical representation of Throughput Vs Speed.

Table 3.8: Speed Vs Throughput

Speed	Throughput(Kbps)	
	HFWOA-Vanet	QMM-Vanet[118]
20	1784	1111
40	992	555
60	594	370
80	446	277
100	346	222

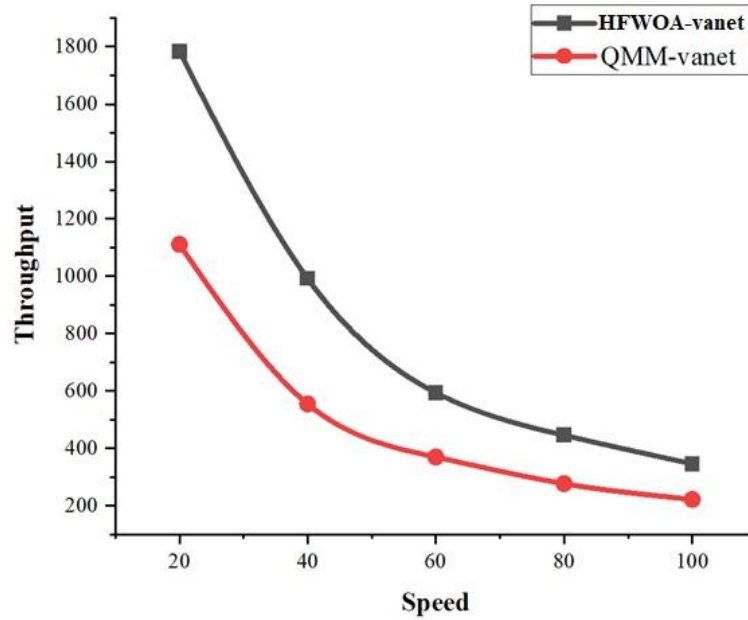


Figure 3.11. Graphical representation for Throughput Vs Speed

The throughput of the existing QMM-Vanet based on Speed is reduced from 1111 to 222. Still, the proposed HFWOA-Vanet is obtained and reduced from 1784 to 346, which proves that the throughput of the proposed technique is higher than the existing technique under Speed. Similarly, the table 3.9 and figure 3.12 are illustrating the graphical representation of Delay time Vs Speed.

Table 3.9:Speed Vs Delay time

Speed	Delay(s)	
	HFWOA-Vanet	QMM-Vanet[118]
20	11.220428	19.27214
40	22.440857	38.544279
60	33.661285	57.816419
80	44.881713	77.088559
100	56.102141	96.360699

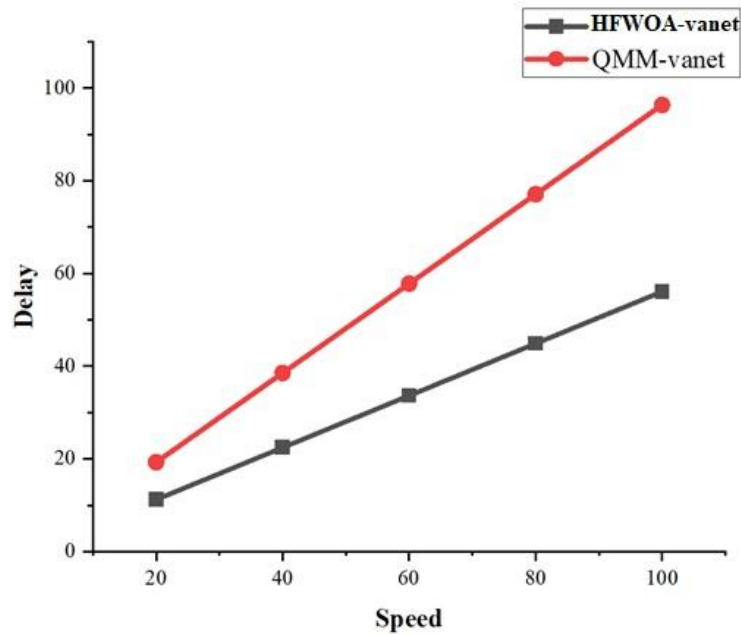


Figure 3.12.Graphical representation for Delay Vs Speed

In the Delay Vs Speed graph (in figure 3.12), the existing QMM-Vanet is increased from 19.27 to 96.36 sec based on speed. But the proposed HFWOA-Vanet is increased from 11.22 to 56.10 sec which is lower than the existing QMM-Vanet technique. Furthermore, the table 3.10 and Fairness Index (FI) Vs. Speed values are represented graphically in figure 3.13.

Table 3.10:Speed Vs Fairness Index

Speed	Fairness Index	
	HFWOA-Vanet	QMM-Vanet[118]
20	4	1.023
40	2	0.8115
60	1	0.641
80	0.8	0.45575
100	0.5	0.2446

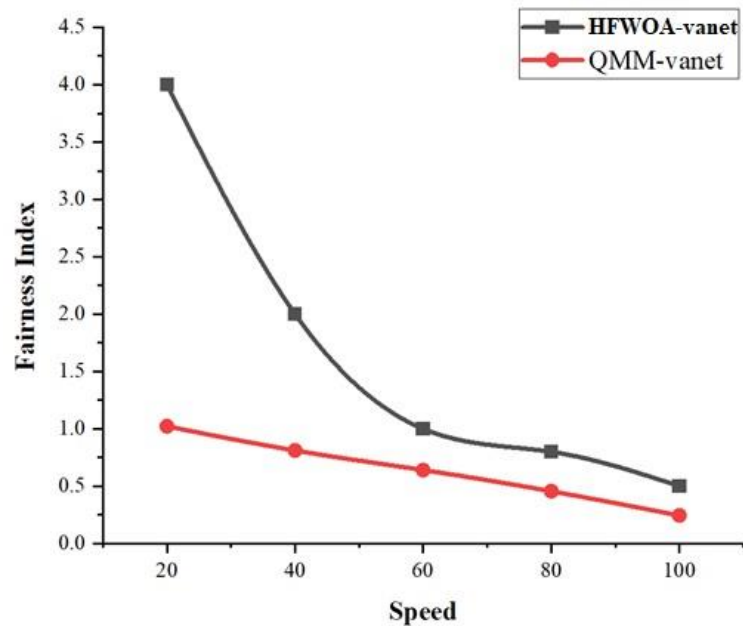


Figure 3.13.Graphical representation for Fairness Index (FI) Vs Speed

From the above diagram (in figure 3.13), the existing QMM-Vanet is decreased from 1.02 to 0.24 based on speed. Still, the proposed technique is decreased from 4 to 0.5 which is also greater than the existing QMM-Vanet technique.

When compared to the current QMM-Vanet technique, the aforementioned analysis showed that the new HFWOA-Vanet technique performs well in all parameters, including energy consumption, drop, throughput, delay, and fairness index (FI) depending on node and speed.

3.6. Summary

This work is based on VANET technology to prevent the malicious behaviour of the vehicle in VANET environment. The incorporation of hybrid technology to enhance the performance of the VANET technology to ensure the self-organized. Meanwhile, it should consider the safety of the vehicles by means of analyzing the vehicles abnormal behaviour. Therefore, the proposed model is developed based on hybrid meta-heuristic technique that incorporated with Firefly Optimization and Whale Optimization Algorithm. The combination of this algorithm is named as a HFWOA-VANET. The HFWOA help to prevent accident and misbehaviour by analyzing the neighbourhood vehicles data. The proposed model is compared with the existing QMM-VANET and it shows that the proposed model is far better than existing technique. The implementation is done in NS2 platform where the performance is analyzed in terms of performance metrics such as Fairness Index (FI), energy consumption, drop, delay, and throughput. Moreover, these parameters are considering in terms of node and speed.

CHAPTER 4

CONGESTION-FREE ROUTING BASED ON A DYNAMIC VANET ENVIRONMENT

4.1 Brief Introduction

A specific type of wireless multi-hop network called a VANET is hampered by rapid topology changes because of the high node mobility. Intervehicle communication is becoming into a potential area for research, standardization, and development as more cars are outfitted with wireless communication and computing technology. Numerous applications are made possible by VANETs, including real-time traffic condition monitoring, blind crossing prevention, safety, dynamic route planning and collision prevention. Providing Internet access to vehicle nodes is another crucial use for VANETs.

4.2 Introduction to VANET Environment

When multiple vehicles broadcast numerous messages at once, data congestion arises in VANETs. The high volume of traffic on the roads, ongoing building projects, accidents, medical emergencies and social events, to name a few are the main causes of congestion. Daily workers who suffer from conditions including infections, vision impairment, skin disorders, allergies and throat illnesses, in addition to their longer journey times, suffer as a result of congestion. Because everyone wants to get where they are going as soon as possible, it also adds to a rise in traffic accidents. If congestion is predicted in advance, commuters can arrange their trip to avoid congested areas, which can be of tremendous help to them. The routes can be chosen either utilizing swarm intelligence, such as Ant Colony Optimization (ACO), Particle Swarm Optimization (PSO), etc., separately or in combination, or by using the usual routing technique that finds the shortest path, i.e., the Dijkstra algorithm. Swarm intelligence algorithms are recommended for these applications since it is a human propensity to desire to travel as quickly as possible [255]. For VANETs, the use of unicast routing presents difficulties in simulating realistic vehicle motion in real city' roadways. Vehicle nodes (VN), On Board Units (OBU)-equipped vehicles, and

permanent nodes known as RSU make up the vehicular network. These RSUs are attached to a roadside infrastructure network that will be accessible to all vehicles. Wireless (ad hoc) methods can be used by OBU and RSU to connect with the vehicles [256].

The majority of these systems use actuated or adaptable signals in an adaptive and non preemptive traffic control mechanism. The main issue with these signals is that no phase in the cyclic order can be avoided; as a result, it will always be given the green light even if there are no vehicles in that phase. This will cause needless delays for the vehicles displayed in earlier rounds. There is a preventative strategy to lower the congestion in VANETs to lessen the delay brought on by the aforementioned circumstance. The hassle-free, smooth mobility of cars is the core objective of VANET. It powers the functionality of VANETs and aids in the development of an effective transportation system when used in conjunction with a number of wireless communications technologies. Due to the vehicle's high degree of mobility, new vehicles may regularly join the network or depart from it. When there are few high-speed cars in a sparse network, this happens quite frequently. Therefore, relying solely on V2V communication is ineffective for realizing the full potential of VANETs [257].

4.2.1 Modes of VANET

- Vehicle-to-Vehicle (V2V): The huge bandwidth millimetre wave (mmWave), which relies on V2V communication between the intra-cluster CVs, has a number of drawbacks, such as poor diffraction and high attenuation. V2V is used to disseminate traffic information among automobiles in vehicular networks for short-range communication. Real-time V2V communication is quick, reliable and secure [258].
- Infrastructure to Vehicle (I2V) has been added as a definition for Vehicle-to-Infrastructure (V2I), also known as "V2X communication" [259]. This makes an effort to reduce the difficulty of computation and the danger of losing secret keys and Infrastructure-to-Infrastructure (I2I).

4.2.2 Basic Structure of VANET

Structure of VANET implies in Fig 4.1. Research on intelligent transportation systems (ITS) has recently shifted its attention to vehicular ad-hoc networks and the next generation of sensing technology (VANET). The potential for distributed real-time traffic variable monitoring has expanded thanks to V2V and V2I wireless communications. Distributed monitoring describes the method by which traffic variables, both large and small, are gathered by moving cars without the use of infrastructure. For the congestion detection issue using VANET, numerous works have been put forth. These methods merely identify congestion. They do not distinguish between recurring and non-recurrent congestion (NRC) causes. They are unable to be used to divide the congestion into its constituent parts. There are still a number of unresolved issues in transportation, despite extensive research into how much of the overall congestion is attributable to NRC for both highway and urban traffic. First of all, NRC occurs at various times and places within an urban road network. With traditional induction loops, cameras and floating cars systems that are expensive to deploy and maintain for wide coverage areas. It becomes challenging to monitor traffic in real time or continuously. To ensure better monitoring of road traffic at different levels of granularity, alternative, flexible and cost-effective methods are required. Secondly, current NRC detection techniques do not operate in real-time and require large datasets. In order to implement relevant preventive actions for returning road congestion to normality, drivers and traffic management facilities can get crucial information about the consequences of the observed NRC in actual.

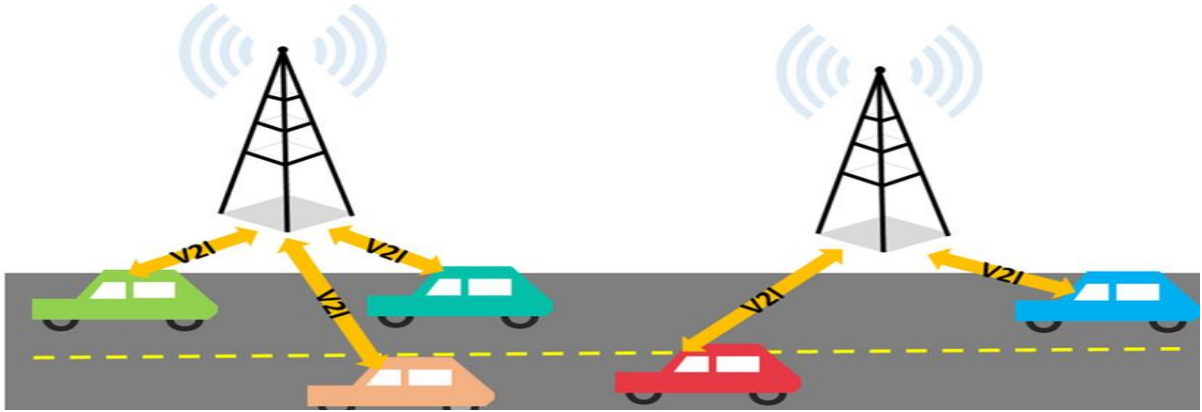


Figure 4. 1: Structure of VANET.

Finally, once an NRC event is discovered, NRC detection methods should be better able to describe it. Existing techniques only measure the impact of the observed NRC in terms of space and time. We should be able to identify the NRC's underlying causes as well [259]. Both social networks and vehicular networks use cellular networks, but as both network entities now depend on one another, interest in both is growing. Due to the difficult needs for information transmission among a large number of users, the necessity for vehicular social networks (VSNs) is created. The answer to providing central data repositories for enormous amounts of data is to use vehicle clouds. It can aid in reducing and regulating dangerous driving and the associated risks. It is also difficult to pinpoint social network traffic hotspots. To model traffic conditions, temporal and spatial chunks of crowd source data are used. It has been determined after analysing many studies that social network traffic is stable. 5G offers dependable low latency communication, just like 4G. The information gathered from social and vehicular networks by FoG servers can be improved in order to anticipate potential dependencies. It blends local decision-making with global distribution aspects in order to decrease latency. [260].

Due to dynamic topology and slow information propagation, VANETs also struggle with connectivity issues, especially early in deployment while RSUs are still being installed. By adding reasonably affordable infrastructure for better information distribution at some

sites in a city region, the issue can be mitigated. These roadside supporting units (RSUs) serve as a backbone network, exchanging information with passing cars and supplying information quickly and readily to distant vehicles. It is possible to average all atomic values across the whole traffic jam zone without suffering a large loss in accuracy. This greatly reduces transmission overhead since only a tiny level of content needs to be delivered. As can be seen, data correlation is essential for data consolidation and the connection factor, but its size relies on the actual volume of traffic and the state of the roads. The accuracy and transmission costs of data aggregation methods must always be balanced, with smaller segment sizes, a better approximation is achievable, but more information must be transmitted [261]. Application latency for VANETs safety applications must be 100 ms and a packet delivery ratio must be less than 90%. The conventional IEEE 802.11 protocols will function well and there won't be any congestion if the VANET's node density is low or below that threshold. This allows VANET to send messages to its nodes and broadcast beacon (every vehicle in the network regularly transmits small data packets called beacons, which include information such as its current position and velocity) messages. Congestion will occur in VANETs if more nodes deliver their messages at the same time. Ten Mega Hertz's first six service channels are reserved for non-safety message broadcast. The second control channel, operating at 10 Mega Hertz, is set aside for the delivery of safety messages and the final channel, operating at 5 Mega Hertz, is reserved for future usage. Low priority messages are transmitted over service channels. Control signals are sent through the channels designated for national priority messages. Dedicated short-range communication has helped to facilitate these communications (DSRC) [262].

4.2.3 DSRC bandwidth

The channel bandwidth for DSRC, divided across 8 channels is shown in Fig 4. 2. Three categories have been established. Ten Mega Hertz's first six service channels are reserved for non-safety message broadcast. The last control channel, at 5 Mega Hertz, is set aside for future applications, while the second control channel, at 10 Mega Hertz, is allocated to the transmission of safety messages. Low priority messages are transmitted over service channels. Control messages are transmitted using the channels set aside for sending

urgent messages. The transmission range and speed range for DSRC is 10 m to 1000 m and 3 Mbps to 27 Mbps, respectively [263].

Table 4.1:DSRC Channel

DSRC Channel								
Service Channel	Service Channel	Service Channel	Control Channel	Service Channel	Service Channel	Service Channel	Reserved Channel	
5.925 Ghz	5.915 Ghz	5.905 Ghz	5.895 Ghz	5.885 Ghz	5.875 Ghz	5.865 Ghz	5.855 Ghz	5.85 Ghz

Vehicles in the data transmission are classified according to their movement, duration, speed and direction, radio frequency, resource limitations, etc. By avoiding the negative effects of the aforementioned traits to facilitate constructive communication, information transmission is accomplished reliably. Three message formats, including data, control and event messages are frequently transmitted in a VANET. The communication protocols make use of the cooperative character of the vehicles to operate data transmission messages.

The internet protocols expressly control the timing and delivery of data and control messages on a regular basis. Event messages on either side are generated without a set time interval and indicate an issue. The density of the vehicles is another significant factor contributing to congestion. The cars randomly adopt the Manhattan mobility model (MMM), which changes the population of an intersection or a highway. When this occurs, the cars flood the channel of communication that is shared and emit control messages or beacons to gather relevant data (such as location, destination route, and cloud connectivity, etc.). Communication problems, connection problems, a delay in message delivery, etc. develop as a result of the overflow of synchronous and asynchronous packets from various vehicles. The link stability feature is another problem for vehicle communication because of

the vehicles' speed and orientation. Unbalanced traffic loads, vehicle characteristics, and the kind of resource constraints on the vehicles all have an effect on how well VANET performs. [264].

4.2.4 Dynamic clustering in VANET

The VANET network communication uses a dynamic network because certain nodes move in an erratic or inconsistent manner usually causing structural deviations. As a result of the network separation, this eventually causes network expiration. The mobility pattern or forecasting pattern can be anticipated in order to increase the device's longevity, which will lead to extensive use of the application in multimedia, commercial, emergency, safety and traffic management applications. Additionally, effective Quality of Service is a must for efficient data transmission (QoS). Therefore, creating a suitable routing system for cars on a big scale is a difficult problem. The sustainability of the network is severely harmed by the issue of network scalability. Delays might also be risky when it comes to monitoring and safety applications. In this context, intelligent clustering algorithms that contribute crucial elements can be developed to optimize vehicular networks for fair distribution of network load and scalability. In order to find the optimum route, five new algorithms are suggested in this study for the VANET environment.

On the other hand, the majority of research in the subject of clustering is focused on the static/traditional clustering method, which groups cars into clusters according to how close they are to the Base Station/Road Side Unit (BS/RSU) that will be chosen as the Cluster Head (CH) [265]. At midnight, there is a very high likelihood that a rural area will have a low vehicle density. Due to the lack of other vehicles, the packet will be lost in this case and the subsequent vehicles' arrival in the accident scene is inevitable. A new hybrid network is the subject of a recent study that seeks to address this serious issue. Researchers are recommending the usage of Wireless Sensor Networks for the deployment of wireless sensors alongside roadways (WSNs). Wireless sensor networks are a developing technology for the future Internet of Things (WSNs). They are frequently employed, including by ITS. WSNs are networks of inexpensive wireless sensor nodes that range in size from medium to

large and are used to collect, process, and distribute data about their environment. Significant cost and distributed intelligence advantages are offered by WSNs. The utilization of inexpensive, wire-free equipment lowers installation and maintenance costs. Diverse real-time traffic safety applications can be created with distributed intelligence which is not possible with centralized systems.

When used in conjunction with other technologies like VANETs, WSNs can be seen as additional elements of a large cluster within the context of ITS. The suggested system is known as a hybrid network of vehicular ad hoc and wireless sensor networks, or VANET-WSN. The proposed VANET-WSN has two types of sensor nodes: roadside sensor nodes which are placed at specified intervals along roadways and vehicular nodes (VN), which are embedded in moving cars (SN). The VNs gather accurate data, such as the position and speed of the vehicles and transmit it to their intended location using additional VNs and SNs [266].

4.2.5 Traffic congestion in VANET

Event-driven architectures (EDAs), a new architectural paradigm, have emerged in recent years to handle a massive volume of events. It is a type of software architecture where events are processed as soon as they are received with the goal of minimizing processing time. EDAs already have a significant impact on numerous industries, including banking and the transportation of products [267]. Also, connectivity reduces the quality of service (QoS) for the permitted vehicles that are within the communication range of the RSU since it uses up the transmission channel and the RSU's limited-service capacity [268]. Data transmission efficiency requires the use of QoS. In situations like safety and surveillance applications, delay might be deadly. One of the issues that seriously undermines a network's ability to remain sustainable is scalability.

The network's load balancing needs to be handled for the duration of the network. Intelligent methods can be quite useful in this situation to improve the efficiency, manageability, scalability and load distribution of the vehicular network. In a network, clustering refers to the arrangement of nodes into groups based on similarities and

differences in order to accomplish certain objectives. By taking into account many factors like the distance between nodes, bandwidth availability, etc., the similarity and unlikeness may be determined [269]. One of the essential requirements of VANET applications for dispersing and diffusing messages is the availability of effective, efficient, and scalable routing protocols. Thus, one of the major problems with VANETs is the lack of a trustworthy and effective routing system. One of the best approaches to deal with the VANET scalability issue is to use hierarchical and clustering strategies. When using a clustering-based technique, data can be sent from cluster member nodes to the cluster head. The cluster head can then eliminate duplicated data using data aggregation techniques [270].

4.3. Congestion-Free Routing Process in VANET

The number of cars on the road has increased exponentially as a result of the regular increasing population in urban areas. Overload caused by vehicular traffic is one of the most significant social and economic issues of our time. Due to the quality growth of many sectors, it is necessary to get to your destination in a fantastic amount of time. Even though important areas are in the same direction, trouble nevertheless occurs. One such example is a single-generation park that houses multiple organizations, each of which produces more than 100 people. The need for a method to prevent automotive traffic congestion arises when travel becomes unavoidable. The demand of the hour is for a smart shipping machine that uses peer-to-peer technology to give real-time data about website visitors. The word for a desire for the improvement of expensive infrastructures or a street form exchange used by the prevailing sophisticated shipping systems. Despite the fact that those structures appear to be incredibly powerful, their deployment will require a significant amount of time and money.

4.4. Background of QOS Routing, HHO and BWO Algorithms:

In the proposed study, the meta-heuristic-based HHO and BWO algorithms were coupled to examine the effects of QoS in the dynamic VANET environment. The HHO and BWO optimization techniques were each described in detail in the section that followed.

4.4.1. HHO algorithm

The mathematical model for the Harris hawk optimization metaheuristic optimization is shown in fig 4.2, which was first proposed in, the cooperative behaviour of Harris hawks when they hunt, chase and besiege their prey. Since there are no gradients in the HHO's population optimization, it has a competitive advantage over other techniques in terms of conversion speed. There are two key stages to the HHO: exploration and exploitation. Additionally, the algorithm switches from exploration to exploitation at a transition period.

$$\sum_{i=1}^{N_*} X_i^*(Iter) \quad (4.1)$$

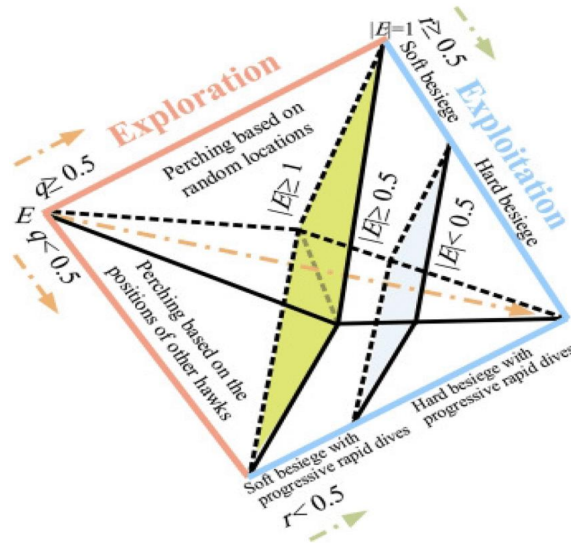


Figure 4.2: HHO algorithm phases of development

In the exploring phase, Harris hawks begin looking for victims at random using the following formula:

$$\begin{aligned} & X^*(Iter + 1) \\ &= \begin{cases} X_{rand}^*(Iter) - R_1 |X_{rand}^*(Iter) - 2R_2 X^*(Iter)| & \text{if } q_* \geq 0.5, \\ (X_{rabit}^*(Iter) - X_m^*(Iter)) - R_3 (LB + R_4 (UB - LB)) & \text{if } q_* < 0.5 \end{cases} \end{aligned} \quad (4.2)$$

$X^*(Iter + 1)$ is where the hawks are in the iteration $(Iter + 1)$, $X_{rabbit}^*(Iter)$ is where the rabbit can be found.

R_1 to R_4 and q_* are arbitrary figures that can range from 0 and 1.

$X_{rand}^*(Iter)$, X_m^* is the average position of the current hawk population as defined by Equation, and represents a hawk that is chosen at random.

$$X_m^*(Iter) = \frac{1}{N_*} \sum_{i=1}^{N_*} X_i^*(Iter), \quad (4.3)$$

X_m^* which hawks are where they are located (solution). Hawks' sizes are indicated by the letters N_* and their locations by the letters X_i^* .

4.4.1.1. Process of exploration to exploitation transition

There are two behaviours which need to be simulated during the exploitation phase shown in Fig. 4.3. First is a soft besiege, when the rabbit's energy is still high and it may move quickly. In this situation, Harris hawks attempt to follow it quietly and keep an eye on it till it begins to tyre. The second behaviour is the harsh besiege, where the prey is exhausted and lacks the energy to flee. In order to launch a swift assault, the Harris hawks in this mode create closed circles.

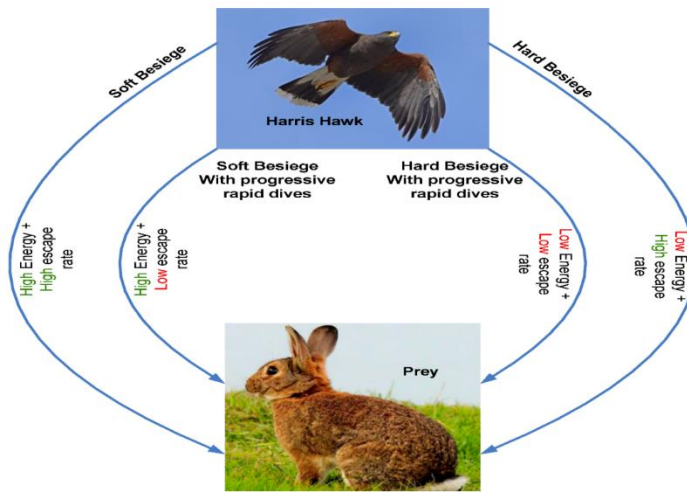


Figure 4.3.: Patterns of prey attack by Harris hawks

The following equation is used to compute the energy of the rabbit in this section:

$$E^* = 2E_0^* \left(1 - \frac{Iter}{T^*}\right), \quad (4.4)$$

E^* = The rabbit's external energy,

T^* = The maximum iteration size,

E_0^* = Energy input from each phase, $-1 < E_0^* < 1$.

The rabbit state is identified by HHO based on the change of E_0^* .

4.4.1.2. Soft besiege

When the soft besiege situation is in effect $R \geq 0$ and $E^* \geq 0$, which is modelled as:

$$X^*(Iter + 1) = \Delta X^*(Iter) - E^* |J^* X_{rabbit}^*(Iter) - X^*(Iter)|,$$

$$\Delta X^*(Iter) = X_{rabbit}^*(Iter) - X^*(Iter), \quad (4.5)$$

where ΔX^* there is a difference in the prey's position.

$Iter$ current location of Hawk in the iteration.

$J^* = 2(1 - R_s)$ refers to the prey's leap height and stage of escape.

R_s represents a random number between 0 and 1.

4.4.1.3. Hard Besiege

Hard besiege condition is valid when $R \geq \frac{1}{2}$ and $|E^*| \geq \frac{1}{2}$.

The prey is worn out and lacks the energy to flee. The following model describes this phase:

$$X^*(Iter + 1) = X_{rabbit}^*(Iter) - E^* |\Delta X^*(Iter)| \quad (4.6)$$

4.4.1.4. Soft Besiege With Progressive Rapid Dive

Valid soft besiege condition is progressive quick dive when $R < 0$ and $|E^*| \geq 0$.

The prey has enough energy at this point to successfully flee. Hawk investigates the following manoeuvre at this level, which can be expressed as follows, for executing gentle besiege:

$$X^*(Iter + 1) = X_{rabbit}^*(Iter) - E^*|\Delta X^*(Iter)| \quad (4.7)$$

Where, $Z^* = Y^* + S^* \times lf(d)$ and

d = Issue dimension,

$S_{1 \times d}^*$ = Random vector along with levy flight.

$$lf(d) = 0.01 \times \frac{\mu^* \times \sigma^*}{|\vartheta^*|^{\frac{1}{b}}} \cdot \sigma^* = \left(\frac{\rho(1+b) \times \sin\left(\frac{\pi b}{2}\right)}{\rho\left(\frac{1+b}{2}\right) \times b \times 2^{\left(\frac{b-1}{2}\right)}} \right) \cdot b = 1.5$$

ϑ^* and μ^* = Amounts that fluctuate between 0 and 1 at random.

Update on the hawk's movements,

$$X^*(Iter + 1) = \begin{cases} Y^* & \text{if } f(Y^*) < f(X^*(Iter)) \\ Z^* & \text{if } f(Z^*) < f(X^*(Iter)) \end{cases} \quad (4.8)$$

4.4.1.5. Process of advanced rapid dives when hard surround:

R is less than 1/2 and $|E^*|$ is less than 1/2,

Given that hawks were present around the rabbit in this work, their actions are modelled here,

$$X^*(Iter + 1) = \begin{cases} Y^* & \text{if } f(Y^*) < f(X^*(Iter)) \\ Z^* & \text{if } f(Z^*) < f(X^*(Iter)) \end{cases} \quad (4.9)$$

$$Y^* = X_{rabbit}^*(Iter) - E^*|J^*X_{rabbit}^*(Iter) - X^*(Iter)|$$

$$Z^* = Y^* + S^* \times lf(d)$$

$$X_m^*(Iter) = \frac{1}{N_*} \quad (4.10)$$

4.4.2.BWO Algorithm

The Black Widow Optimization Algorithm (BWO) was developed as a result of the distinctive mate-finding habits of black widow spiders. Cannibalism is a unique step in this process. This stage results in early convergence because species with poor fitness are excluded from the circle. To evaluate the effectiveness of the BWO algorithm in locating the most effective solutions to the problems, 51 various benchmark functions are employed.

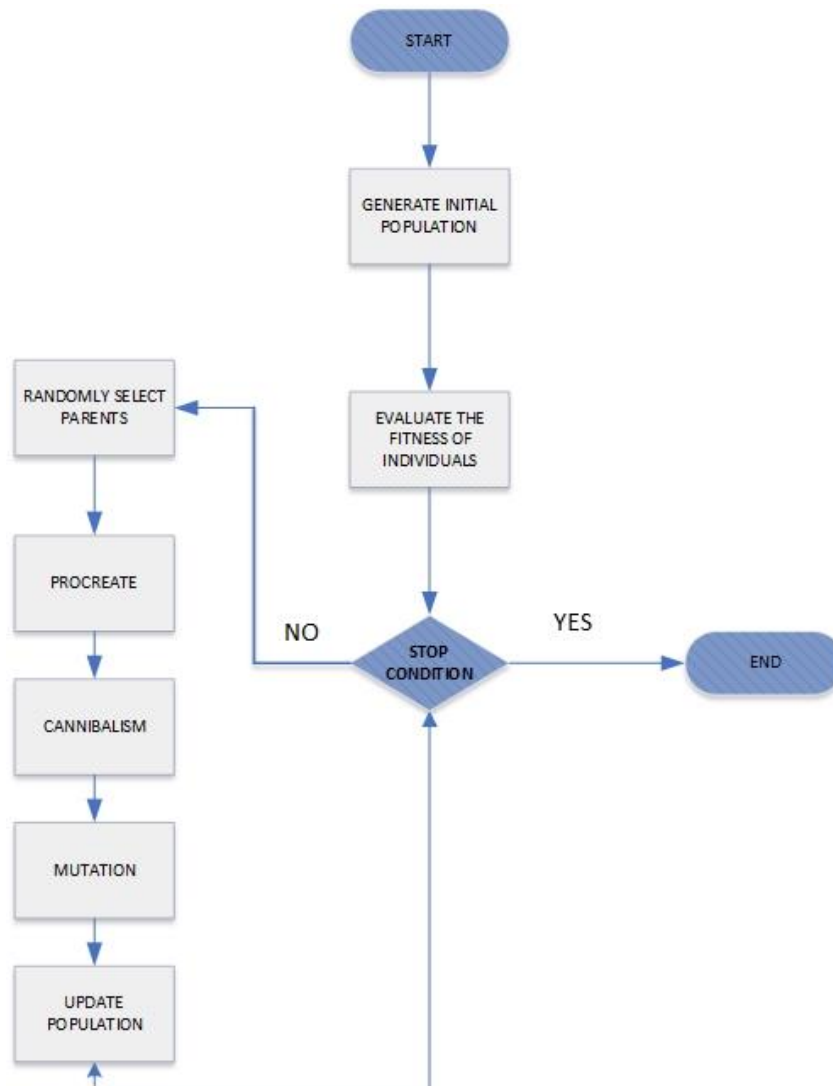


Figure 4.4: Flowchart of BWO

Since each spider in the proposed algorithm represents a potential solution, the algorithm begins with a population of initial spiders. These original spiders attempt to reproduce the next generation in pairs. After or during mating, the female black widow consumes the male. Then she discharges the eggs she has accumulated in her reproductive level of functioning into the egg sacs. Spiderlings emerge from egg sacs as early as 11 days after being placed. For a few days to a week, they live together on the maternal web, at which time sibling cannibalism is seen. After that, they fly away on the wind. Fig 4.4 shows the steps of BWO.

4.4.2.1. Initial population

A Black widow spider has been used in the Black widow Optimization Algorithm (BWO) to represent each possible solution to a problem. The values of the variables causing the problem are displayed on each Black Widow spider. In this study, the structure should be regarded as an array in order to solve benchmark functions.

A widow is an array of $1 * M_{VAR}$ values that represents the answer to an M_{VAR} dimensional optimization problem. Here is how this array was defined:

$$Widow = [i_1, i_2 \dots \dots M_{VAR}] \quad (4.11)$$

Each of the variable values ($i_1, i_2 \dots \dots M_{VAR}$) is floating-point number. The fitness of widow is obtained by evaluation of fitness function ff at a widow of ($i_1, i_2 \dots \dots M_{VAR}$). So,

$$Fitness = ff(widow) = ff(i_1, i_2 \dots \dots M_{VAR}) \quad (4.12)$$

A candidate widow matrix of size $M_{POP} * M_{VAR}$ is produced with an initial population of spiders to begin the optimization method. After mating, pairs of parents are chosen at random to carry out the procreation step, during which the female black widow consumes the male black widow.

4.4.2.2. Procreate

The pairs begin to mate independently of one another in order to generate the next generation. This is similar to how it happens in nature, as each pair mates in its own web, apart from the others. In the actual world, each pairing produces about 1000 eggs, although some of the spider offspring do survive and are stronger. Now, in this technique, in addition to the widow array holding random numbers, an array named beta needs also be formed in order to replicate then offspring is produced by using β with the following equation in which i_1 and i_2 are parents, j_1 and j_2 are offspring.

$$\begin{cases} j_1 = \beta * i_1 + (1 - \beta) * i_2 \\ j_2 = \beta * i_2 + (1 - \beta) * i_1 \end{cases} \quad (4.13)$$

Repeating this technique $M_{VAR}/2$ times should prevent duplication of the randomly chosen numbers. The mother and offspring are then added to an array and sorted by fitness value; some of the best people are then added to the newly created population in accordance with the cannibalism grade. Every couple must follow these steps.

4.4.2.3. Cannibalism

Here, cannibalism takes three different forms. The first one involves a female black widow eating her spouse during or after mating, which is known as sexual cannibalism. We could distinguish between male and female using this algorithm based on their fitness levels. Sibling cannibalism is another type, where the stronger spiderlings eat their weaker siblings. In this technique, the number of survivors is calculated based on a cannibalism rating (CR). The third type of cannibalism, in which the young spiders consume their mother, is occasionally seen. To identify whether spiderlings are strong or weak, we use the fitness value.

4.4.2.4. Mutation

At this point, we choose a random sample of Mutepop people from the population. Each of the selected options swaps two array elements at random. The mutation rate is used to compute mutepop.

4.4.2.5. Convergence

Three stop criteria are comparable to those of other evolutionary algorithms:

(A) a set amount of iterations.

(B) Observing that the fitness value of the best widow has remained constant across several rounds.

(C) Achieving the required degree of accuracy

4.4.3. QOS in VANET Networks

The ability of a network to provide applications with a certain degree of service is referred to as QoS. In VANET networks, QoS is calculated in accordance with the supported applications. Applications for the VANET that fall under various limitations include those for traffic monitoring, comfort and road safety. The authenticity of real-time information is the major restriction for programmes that monitor traffic and road safety. Solutions for comfort, however, demand constant communication. The cooperation of many network elements, such as a QoS routing algorithm, a resource reservation system, and a Media Access Control (MAC) layer, is necessary for the QoS solution for VANETs. Since QoS routing techniques enable the network layer, which is the main technology for delivering QoS. The seeming main goal is to make sure a network does have the ability to deliver the desired results.

- **DELAY-** The delay is the most crucial factor taken into account by routing methods. It alludes to the processing, propagation, transmission and access delays. The average amount of time between a node's attempt to launch a packet and the time for system is high and is known as access delay or queuing delay. The time to submit an online packet would be during the transmission delay. The median travel time between transmitting and receiving a packet is known as the propagation delay. After being validated by the endpoint, a message must wait in the target queue before being forwarded to the destination. This is referred to as a processing delay.

- **DISTANCE**- It refers to the physical separation between the current node and the following forwarding neighbour node. The most frequently utilized fundamental parameter is distance.
- **LINK RELIABILITY**- In highly dynamic networks like VANET, communication channels are extremely susceptible to disconnecting. Therefore, particular consideration must be given to these networks' routing reliability. Link reliability is the likelihood that a direct communication link will be active continuously for a certain amount of time between two nodes.
- **SECURITY** - Wireless networks that try to provide services with security and QoS assurances must have algorithms for secured QoS routing.
- **HOP COUNT** - The "hop count" or "number of hops" refers to the number of connections that are used to distribute resources along the path between the destination and source nodes.
- **NEIGHBOUR NODES** - A node has a number of one-hop nodes within its transmission range. Neighbor nodes are the name given to these one-hop nodes. By exchanging the Hello message, they update their statuses, including their position, current time, speed, and direction. A node and its neighbours move randomly and frequently change locations in a dynamic mobile ad hoc network. The quality of neighbours is hence one consideration to make in order to enhance the performance of routing systems.
- **ENERGY** - This number shows a node's capacity at the start of the network deployment. Routing protocols that are energy-conscious are designed to lengthen the life of networks.
- **MOBILITY**- Due to nodes' high mobility in wireless mobile networks like VANETs, there are frequent topological changes and network dispersion.
- **STREET CONNECTIVITY**- The term "street connectivity" describes the density and directness of linkages within street networks. When creating a routing protocol for a mobile adhoc network, street connectivity is a crucial factor.

4.5. Hybrid-Harris Hawks-Black Widow based VANET (H-HHBW-VANET)

In this section, the improved routing protocol is explained. Figure 4.5 demonstrates the flow chart of the improved routing protocol H-HHBW-VANET. In this flowchart, the BWO algorithm is combined with HHO for getting a more optimal solution. Using this improved routing protocol H-HHBW-VANET, the CH and CMs are selected. Here, the parameters of the vehicles and the HHO are initialized then calculate the fitness of each vehicle and update the energy value of the rabbit. If the energy of the rabbit is greater than the one means the HHO takes the exploration process otherwise it takes the exploitation process depending upon the rabbit's dives. The position of the rabbit is taken as the best position and in the population-based on the fitness function, updates the prey's location. Hawks are considered as the source and forwarding vehicle and prey are considered as the destination vehicle. Then compare the vehicles' QoS performance matrices, the vehicle with better QoS value which is selected for CH which is repeated until all the vehicles in the clusters are updated. The QoS value is incorporated with vehicles' speed, velocity, distance, the number of neighbour vehicles, and throughput. All the vehicles in the cluster have these parameters which help to elect the CH and CMs, the optimal solution is driven by this H-HHBW-VANET. The H-HHBW-VANET with improved routing protocol effectively detects the routing of the cluster nodes and reducing the congestion between the nodes. The proposed H-HHBW has more superior optimization than the HHO, BWO algorithms, and other optimization techniques.

In the phase of initialization of all the solution areas initial hawks' population and the vehicle's parameters such as distance, speed, velocity, number of neighbor nodes and throughput. This H-HHBWO-VANET is used to improve the QoS performance matrices, to select the CH and CM and to detect an effective congestion-free node routing process in the dynamic VANET environment. The population contains the multiple numbers of vehicles they are,

$$V_1, V_2, \dots, V_n \quad (4.14)$$

The hawks are considering as the source vehicle and the prey (rabbit) is considered as the destination vehicle. The source vehicle is tracking the destination vehicle and the forwarding vehicles by this HHO. The source vehicle is denoted as V_{sh} . The fitness of all the vehicles is calculated in this phase and the fitness of the i^{th} vehicle,

$$F(V_i) = \{\sum D^*, S^*, V^*, T^*, s, p\} \quad (4.15)$$

D^* = The distance of the vehicles,

S^* = Speed of the vehicles,

V^* = Velocity of the vehicles,

T^* = Throughput of the vehicles,

s = State of the vehicle,

p = Availability of channel or Availability of path (route).

$$s = \frac{T^* + dr^*}{d^*} \quad (4.16)$$

Here T^* is represented as the throughput, dr^* is represented as data rate, the delay is denoted as d^* . This is the deciding factor of fitness computation.

The hawks' average location is formulated in the exploration phase as

$$V_{ia}(I_c) = \frac{1}{n} \sum_{j=1}^n V_{ia}(I_c) \quad (4.17)$$

I_c = Current Iteration;

In addition, the energy of the vehicle (prey) is updated and the exploration and exploitation process is established depending on the energy of the prey (vehicle). The CH is selected by comparing the QoS values of each vehicle(node), the maximum QoS value vehicle is selected to the CH. This selection of CHs and CMs are continuing until analyzing the QoS of all vehicles (until the maximum iteration is reached in HHO). The location of the vehicle is updated for each iteration, When the current iteration is greater than the maximum iteration or equal to the maximum, update the best location (best route) using the below equation,

$$V_i(I_c + 1) = \begin{cases} \beta & \text{if } F(\beta) < (V_i(I_c)) \\ d_i & \text{if } F(d_i) < (V_i(I_c)) \end{cases} \quad (4.18)$$

β = The next moving step of the vehicle

d_i = Movement of the source vehicle.

If the current iteration is greater than the maximum iteration, the position of the destination vehicle and forward vehicles are determined is considered the best solution which is the best congestion-free route or location otherwise, it will take the energy updating step of the HHO algorithm. In order to get a more optimal best location, the BWO algorithm is incorporated with HHO to enhance the optimal solution. Therefore, the BWO algorithm widow population is initialized and fitness values are calculated by this. In which the strongest widow (node) is the best solution until the maximum iteration is achieved process is continue. Then finally analyze the QoS performance matrices such as throughput, delay, energy consumption, drop, fair index of each vehicle, and finding the best r routing for effective congestion-free nodes.

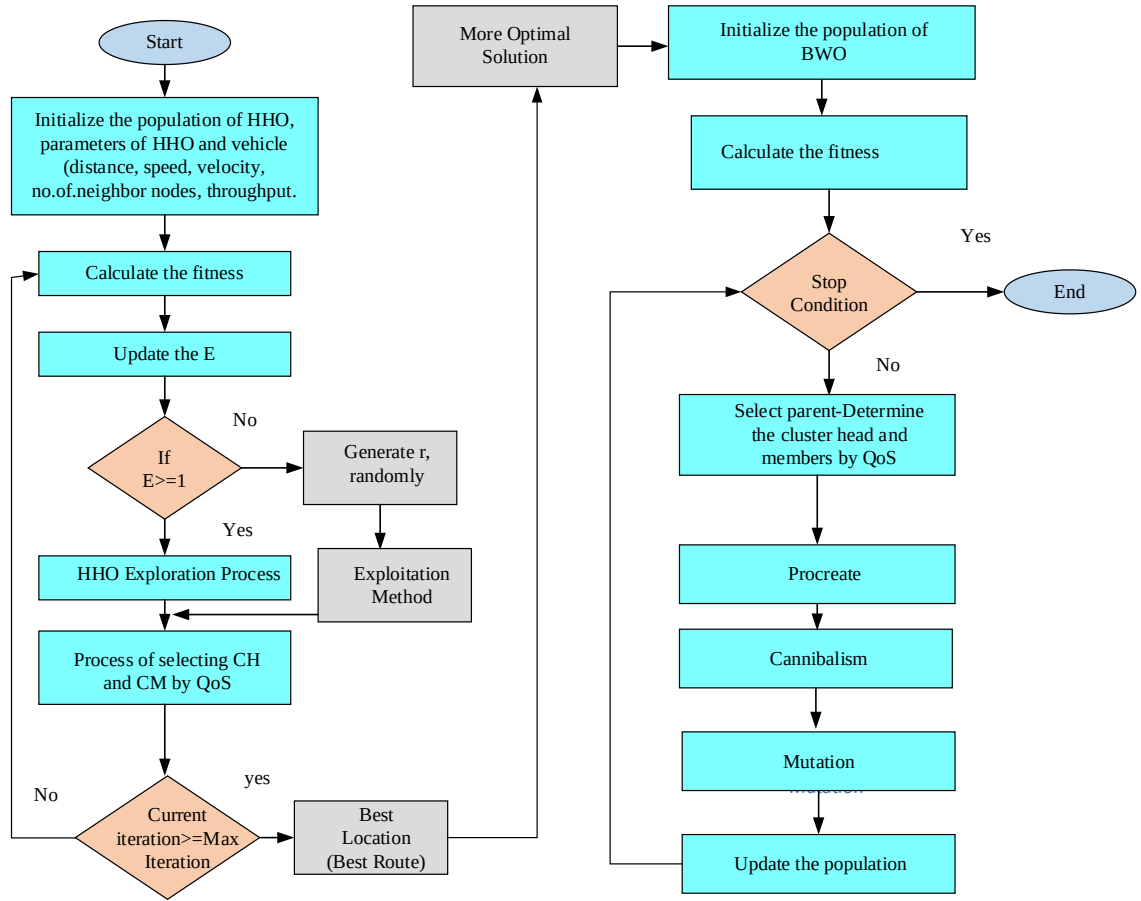


Figure 4. 5: Flowchart of the H-HHBW-VANET

The following section gives a detailed explanation of the results using the proposed approach and proves the proposed approach H-HHBW-VANET is effective by compared with other techniques.

4.6.Results and discussions

In this section, the results are thoroughly explained using QoS performance matrices including Drop, Delay, Energy consumption, Throughput, and Fairness Index (FI). The findings are completed on the NS2 framework and these performance metrics are used to assess the considerable impact of the suggested approaches QoS. Additionally, the suggested hybrid method is contrasted with the current methodology and the outcomes are clearly summarized for all QoS matrices. H-HHBW-VANET is the proposed approach while the HFWOA-VANET, BWO and HHO are used to analyze the findings in two situations based on node and speed-based data. The outcomes of the performance matrices in two situations were explained in the section that followed.

Following are the parameters that were considered all through the evaluation:

- Drop
- Delay
- Energy consumption
- Throughput
- Fairness Index (FI)

Below is a discussion of these parameters, their graphical representation and their range of values.

4.6.1 Performance Metrics

Using the parameters listed below, the proposed technique's performance metrics are compared to those of the existing techniques.

1) Drop

By packet drop, the total number of data packets that failed to reach their destination is shown. Overload, malfunctioning hardware, queue overflow and other factors may be at blame for packet drops. By requiring more time and capacity to transmit a packet, packet drops have an impact on the network's performance. Higher protocol performance is indicated by a lower packet drop rate.

$$Drop = \frac{SP-RP}{SP} \quad (4.19)$$

RP refers to received packets

SP refers to send packets

2) Delay

The time discrepancy between a packet's anticipated arrival time and its actual arrival time is referred to as the delay. A packet experiences delays as it moves from its origin to the destination. The average backoff slot count and successful transmission time following priority assignment determine the delay. When there is no attack on nodes, the latency is smaller, but when a solution is offered, the delay increases since we are using a new path to transmit the packet. To get the packet to its intended node is the goal.

$$D = T_w + T_b + T_t \quad (4.20)$$

T_w is withdrawal time.

T_b is freezing back off time.

T_t is successful Transmission period.

3) Energy Consumption

It calculates the typical amount of energy used by mobile nodes during the transmission operation. When compared to the suggested approach, this increases usage in packet dropping attacks. Regardless of their status, all nodes require the same amount of energy during the simulation.

$$EC (joules) = \sum_{j=1}^n (X_j - Z_j) \quad (4.21)$$

X_j is the initial node energy already present j

Z_j leftover node energy j at end of simulation

n indicates the node of numbers.

4) Throughput

It is stated that the throughput per centre point is the average time for the number of bits that can be delivered from each centre point to its target. The throughput of a framework is the sum of the per-centre point throughput over all of the centre points. By dividing the total number of bundles obtained by the entire simulation duration, the throughput is computed. On a communication network or network node, throughput is the average number of successfully delivered data packets. In other words, throughput is defined as the ratio of total packets delivered to total packets received at the destination. Throughput is typically measured in bits per seconds (bps or bit/s), megabits per seconds (Mbps or gbps), or gigabits per seconds (Gbps).

$$TP(sec) = \frac{Packetreceived * Packetsizes}{(Totalsimulationtime)} \quad (4.22)$$

TP refers to Throughput.

5) Fairness Index

The fairness index is a performance indicator used to equally distribute system resources among nodes. It demonstrates that a high vehicle density causes the fairness index value to decline. This implies that as the level of disagreement rises, protocol fairness declines. The fairness index is a useful metric for assessing how well the schedulers are doing. It comprises of nodes sharing resources. With an increase in vehicle density, the fairness index value rises proportionately. This is because there are more opportunities to create a new link for the subsequent data transfer when there is a high vehicle density.

$$FI = \frac{\sum_K TH_K}{M \sum_K TH_j^2} \quad (4.23)$$

Case 1: Analyze the Node-based performance matrices:

This section explains the performance matrices for the proposed scheme and existing techniques for the QoS based on Node findings. Table 4.2 shows the outcomes of the suggested research in comparison to currently used techniques like HFWOA-VANET, BWO-VANET, and HHO-VANET.

Table 4.2: The performance matrix of the existing method and the suggested model is built on Node

Performance Parameters	Techniques	Nodes				
		20	30	40	50	60
Delay(s)	H-HHBW-VANET[Proposed2]	0.422682	0.584858	0.845636	0.810469	0.963607
	HFWOA-VANET[Proposed1]	0.482682	0.654858	0.905636	0.910469	1.063607
	BWO-VANET[166]	0.553047	1.059783	0.961704	1.228869	1.683063
	HHO-VANET[301]	0.513047	0.689783	0.921704	1.028869	1.183063
Drop(%)	H-HHBW-VANET[Proposed2]	0.984475	0.986718	0.97245	0.978949	0.974986
	HFWOA-VANET[Proposed1]	0.994475	0.989718	0.98245	0.988949	0.984986
	BWO-VANET[166]	0.995541	0.995136	0.994307	0.994082	0.993053
	HHO-VANET[301]	0.996241	0.996136	0.995207	0.994582	0.993653
Energy consumption(Joules)	H-HHBW-VANET[Proposed2]	98	98	97	96	96
	HFWOA-VANET[Proposed1]	98.5	98.5	97.5	97	97
	BWO-VANET[166]	100	100	99	99	99
	HHO-VANET[301]	99	99	98	98	98
Throughput(Kbps)	H-HHBW-VANET[Proposed2]	27964	28749	32403	23760	24717
	HFWOA-VANET[Proposed1]	20196	20763	23402	22308	21097
	BWO-VANET[166]	19349	19334	19165	18921	17100
	HHO-VANET[301]	19749	19634	19465	19121	18100
Fairness Index (FI)	H-HHBW-VANET[Proposed2]	8	6	5	4	4
	HFWOA-VANET[Proposed1]	6	4	3	2	2
	BWO-VANET[166]	2.8698	1.577867	1.4915	0.90784	0.482

	HHO-VANET[301]	3.8698	2.577867	2.4915	1.90784	1.482
--	-----------------------	--------	----------	--------	---------	-------

In Table 4.2, proposed H-HHBW-VANET achieves 0.422682 in delay, 0.984475 in Drop, 98 in Energy Consumption, 27964 in Throughput, 8 in Fairness Index at the node 20th. In addition, 0.584858 in Delay, 0.986718 in Drop, 98 in Energy Consumption, 28749 in Throughput, 6 in Fairness Index at the node 30th. In node 40th, proposed achieves 0.845636 in Delay, 0.97245 in Drop, 97 in Energy Consumption, 32403 in Throughput, 5 in Fairness Index. In 50th node, 0.810469 in Delay, 0.978949 in Drop, 96 in Energy Consumption, 23760 in Throughput, 4 in Fairness Index. For the 60thnode, the following values are achieved: 0.963607 for delay, 0.974986 for drop, 96 for energy consumption, 24717 for throughput, and 4 for the fairness index.

For the existing HFWOA-VANET, the 20thnode achieves 0.482682 in delay, 0.994475 in Drop, 98.5 in Energy Consumption, 20196 in Throughput, 6 in Fairness Index. Additionally, 0.654858 in Delay, 0.989718 in Drop, 98.5 in Energy Consumption, 20763 in Throughput, 4 in Fairness Index at the node 30th. Likewise, 0.905636 in Delay, 0.98245 in Drop, 97.5 in Energy Consumption, 23402 in Throughput, 3 in Fairness Index for the node 40th. Also, 0.910466 in delay, 0.988949 in drop, 97 in energy use, 22308 in throughput, and 2 in fairness index for the 50thnode. The 60thnode achieves 21097 in throughput, 97 in energy usage, 1.063607 in delay, and 0.984986 in drop, as well as 2 in fairness index.

Similarly, 0.553047 in delay, 0.995541 in drop, 100 is obtained in energy consumption, 19349 in throughput, and 2.8698 in fairness index for the 20thnode in the existing BWO-VANET. 1.059783 in delay, 0.995541 in drop, 100 in energy consumption, 19334 in throughput, and 1.57787 in fairness index in the node 30th. For the 40th node, 0.961704 in delay, 0.99307 in drop, 99 in energy consumption, 19165 in throughput, 1.4915 in fairness index. The 50th node has a delay of 1.228869, a drop of 0.994082, an energy consumption of 99, a throughput of 18921, and a fairness index of 0.90784. 1.683063 in delay, 0.993053 in drop, 99 in energy use, 17100 in throughput, and 0.482 in fairness index for the 60thnode.

Similar to the existing HHO-VANET, for the 20th node, the following metrics were recorded: 0.513047 delay, 0.996241 drop, 99 energy consumption, 19749 throughput, and 3.8698 fairness index. The 30th node's metrics for delay, drop, energy use, throughput, and fairness index are 0.689783, 0.996736, 99, 19634 and 2.577866, respectively. For the 40th node, 0.921704 is delay, 0.995207 is drop, energy consumption is 98, throughput is 19465, 2.4915 in fairness index. For the node 50th, 1.028869 is delay, 0.994582 in drop, 98 is energy consumption, 19121 in throughput, and 1.90784 in fairness index. For the 60th node, 1.183063 in delay, 0.993653 in drop, 98 is energy consumption, 18100 in throughput, 1.482 is fairness index.

4.6.2. Performance matrices based on Node are compared

This section compares the suggested approach, H-HHBW-VANET, with the existing approaches and discusses the findings that were obtained using nodes. Below is an example of how Node and delay are represented graphically.

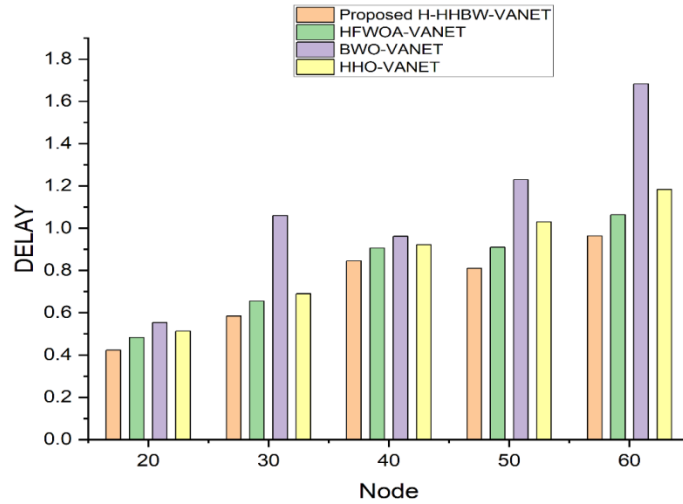


Figure 4.6: The graphical representation of Node Vs Delay

Figure 4.6 shows that when compared to earlier efforts like HFWOA-VANET, BWO-VANET, and HHO-VANET based on the Node, the suggested technique has a short delay time.

Figure 4.7 shows a graphic representation of the Node Vs drop relationship, and it shows that the proposed H-HHBW-VANET has a low drop level in comparison to existing approaches.

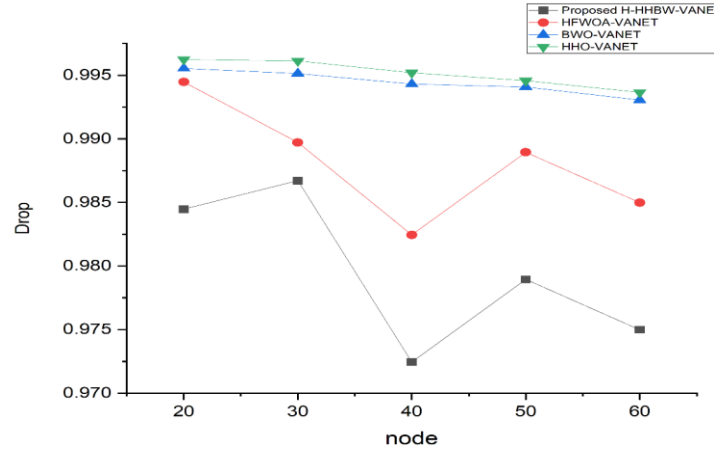


Figure 4.7: The graphical representation of Node Vs Drop

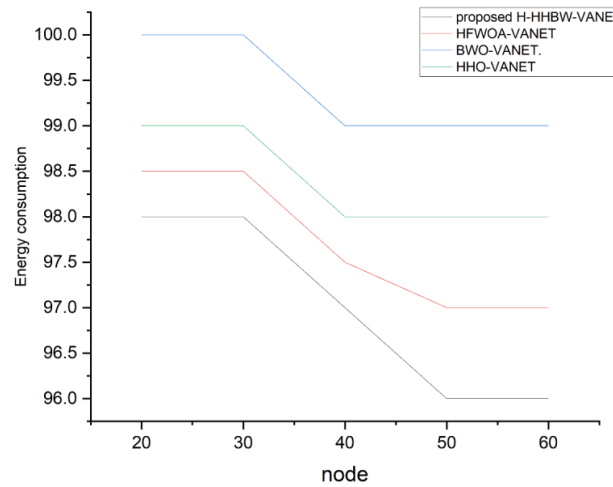


Figure 4.8: The graphical representation of Node Vs Energy consumption

Figure 4.8 illustrates the graphical representation of the Node Vs Energy consumption. Figure 4.8 shows that when compared to existing systems like HFWOA-VANET, BWO-

VANET, and HHO-VANET based on Node, the proposed method H-HHBW-VANET uses less energy.

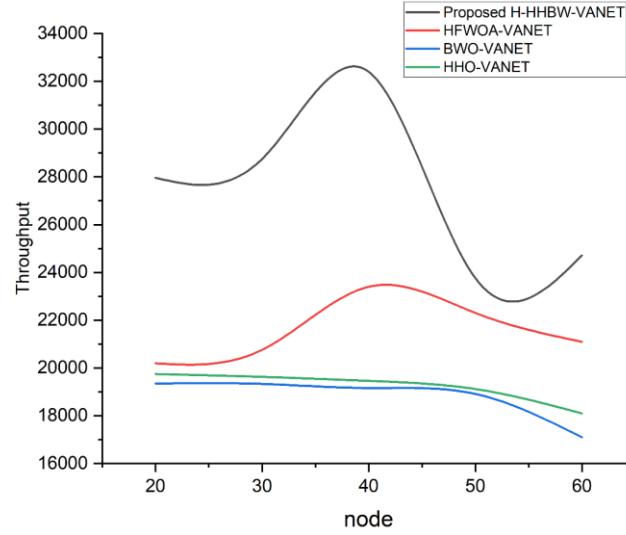


Figure 4.9: The graphical representation of Node Vs Throughput

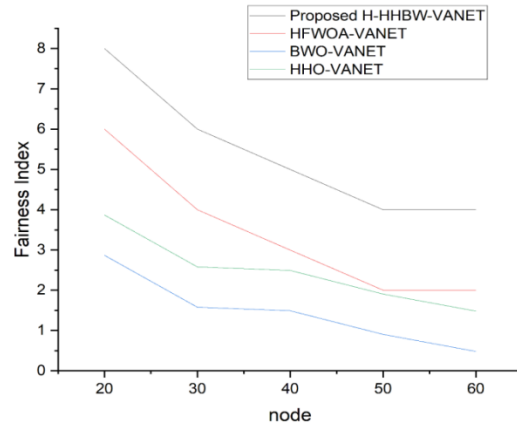


Figure 4. 10: The graphical representation of Node Vs Fairness Index

Figure 4.9 shows a graphic illustration of the Node Vs Throughput relationship. According to figure 4.9, the projected throughput is higher than what is currently being done. The comparison of the fairness indices of the proposed and existing works based on Node is also

shown in figure 4.10. When compared to other methods, the suggested method has a high fairness index, as shown in figure 4.10.

4.6.3. Analyze the performance matrices based on Speed

This section explains the performance matrices for the proposed technique and existing techniques for the QoS based on speed findings. Table 4.3 shows the outcomes of the planned research in comparison to already-in-use techniques like HFWOA-VANET, BWO-VANET, and HHO-VANET.

Table 4.3: The performance matrices of the proposed approach and existing approach based on Speed

Performance Parameters	Techniques	Speed				
		20	40	60	80	100
Delay(s)	H-HHBW-VANET(Proposed2)	10.220428	15.440857	25.661285	32.881713	44.102141
	HFWOA-VANET(Proposed1)	11.220428	22.440857	33.661285	44.881713	56.102141
	BWO-VANET[166]	19.27214	38.544279	57.816419	77.088559	96.360699
	HHO-VANET[301]	25.27214	40.544279	60.816419	80.088559	99.360699
Drop(%)	H-HHBW-VANET(Proposed2)	15.499727	30.999454	43.499181	65.998908	85.498635
	HFWOA-VANET(Proposed1)	19.499727	38.999454	58.499181	77.998908	97.498635
	BWO-VANET[166]	19.873056	39.746111	59.619167	79.492222	99.365278
	HHO-VANET[301]	21.873056	42.746111	63.619167	81.492222	103.365278
Energy consumption(Joules)	H-HHBW-VANET(Proposed2)	1840	2780	4320	5760	7700
	HFWOA-VANET(Proposed1)	1940	3880	5820	7760	9700
	BWO-VANET[166]	1980	3960	5940	7920	9900
	HHO-VANET[301]	2580	4560	6840	8520	10500
Throughput(Kbps)	H-HHBW-VANET(Proposed2)	1954	1092	794	646	546

	HFWOA-VANET(Proposed1)	1784	992	594	446	346
	BWO-VANET[166]	1111	555	370	277	222
	HHO-VANET[301]	911	455	270	177	122
Fairness Index (FI)	H-HHBW-VANET(Proposed2)	5	3	2	1.8	1.5
	HFWOA-VANET(Proposed1)	4	2	1	0.8	0.5
	BWO-VANET[166]	1.023	0.8115	0.641	0.45575	0.2446
	HHO-VANET[301]	0.923	0.6115	0.541	0.35575	0.1446

In table 4.3, For the proposed H-HHBW-VANET, for speed 20th, 10.220428 is delay, 15.499727 is drop, 1840 is energy consumption, 1954 in throughput, 5 in fairness index. Also, 15.440857 in delay, 30.999454 in drop, 2780 in energy consumption, 1092 in throughput, 5 in fairness index for 40th speed. For 60th speed, 25.661285 in delay, 43.499181 in drop, 4320 in energy consumption, 794 is throughput, 2 is fairness index. For 80th speed, 32.881713 in delay, 65.998908 in drop, 5760 in energy, 646 in throughput, 1.8 in fairness index. For 100th speed, delay is 44.102141, 85.498635 in drop, 7700 in energy consumption, 546 in throughput, 1.5 in fairness index.

Similarly, the existing HFWOA-VANET, for 20th speed, 11.220428 in delay, 19.499727 in drop, 1940 in energy consumption, 1784 in throughput, 4 in fairness index. The following statistics are for the 40th speed: 22.440857 in delay, 38.999454 in drop, 3880 in energy, 992 in throughput, and 2 in fairness index. For 60th speed, 33.661285 in delay, 58.499181 in drop, 5820 in energy consumption, 594 in throughput, 1 in fairness index. For 80th speed, 44.881713 in delay, 77.998908 in drop, 7760 in energy consumption, 446 in throughput, 0.8 in fairness index. For 100th speed, 56.102141 in delay, 97.498635 in drop, 9700 in energy consumption, 346 in throughput, 0.5 in fairness index.

For BWO-VANET, for 20th speed, 19.27214 in delay, 19.873056 in drop, 1980 in energy consumption, 1111 in throughput, and 1.023 in fairness index. For 40th speed,

38.544279 in delay, 39.746111 in drop, 3960 I energy consumption, 555 in throughput, 0.8115 in fairness index. For 60th speed, delay is 57.816419, 59.619167 in drop, energy consumption is 5940, 370 in throughput, 0.641 in fairness index. For 80th speed, 77.088559 in delay, 79.49222 in drop, 7920 in energy, 277 in throughput, 0.45575 in fairness index. For 100th speed, 96.360699 is delay, 99.365278 is drop, energy is 9900, 222 in throughput, 0.2446 in fairness index.

For HHO-VANET, for 20th speed, 25.27214 in delay, 21.87056 in drop, 2580 in energy consumption, 911 in throughput, 0.923 in fairness index. For 40th speed, 40.544279 in delay, 42.746111 in drop, 4560 in energy consumption, 455 in throughput, 0.6115 in fairness index. For the 60th speed, there was a 60.816419 delay, a 63.619167 drop, 6840 energy, 270 throughput, and a 0.541 fairness index. For 80th speed, 80.088559 in delay, 81.492222 in drop, 8520 in energy consumption, 177 in throughput, 0.35575 in fairness index. For 100th speed, 99.360699 in delay, 103.360699 in drop, 10500 in energy consumption, 122 in throughput, and 0.1446 in fairness index.

4.6.4. Comparative analysis of the performance matrices based on Speed

This section discussing the comparative analysis of the proposed approach H-HHBW-VANET with the existing approaches such as HFWOA-VANET, BWO-VANET, and HHO-VANET, in addition, the results are attained based on speed. Figure 4.11 illustrates how speed and delay are represented graphically. When compared to the current work, such as HFWOA-VANET, BWO-VANET, and HHO-VANET, the suggested work, as shown in figure 4.11, has a low delay value. The proposed method, H-HHBW-VANET, has a low delay value when compared to other current techniques, such as HFWOA-VANET, BWO-VANET and HHO-VANET based on Speed, as shown in Figure 4.12's graphical representation of the speed Vs drop.

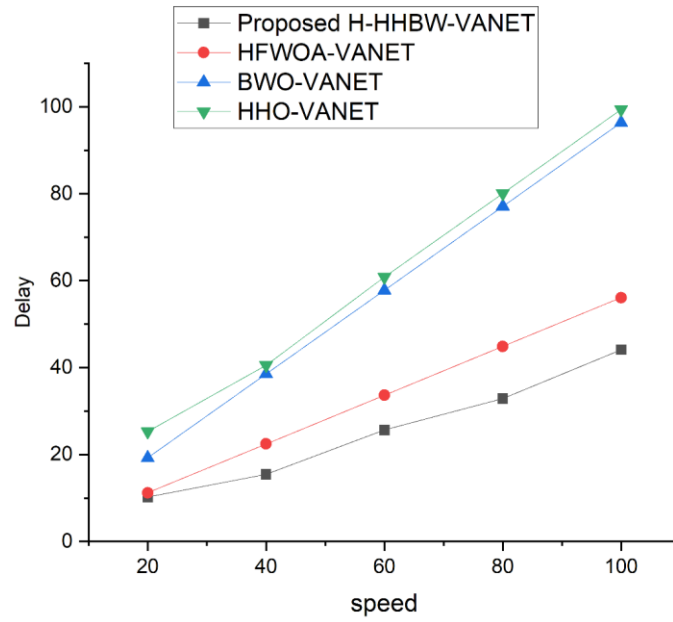


Figure 4.11: The graphical representation of Speed Vs Delay

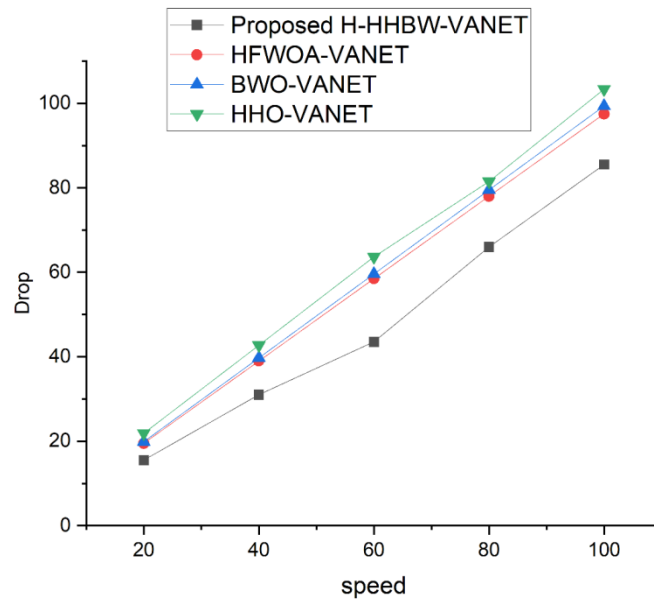


Figure 4.12: The graphical representation of Speed Vs Drop

The graphical representation of the energy usage with speed is shown in Figure 4.13. According to figure, when compared to other strategies based on speed, the suggested method uses less energy.

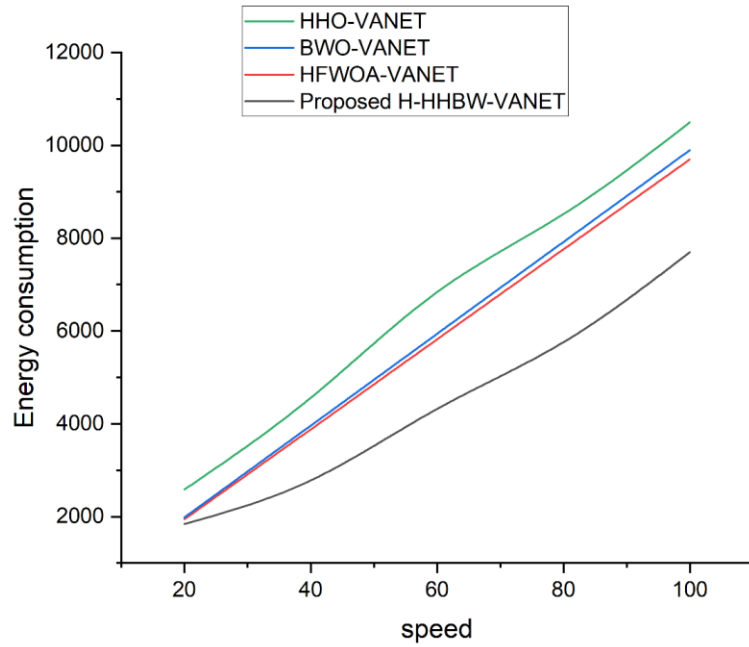


Figure 4.13: The graphical representation of Speed Vs Energy consumption

Figure 4.14 plots Speed Vs Throughput graphically, and when compared to the existing techniques, the proposed work has a high throughput number. Figure 4.15 also shows a graphic representation of the fairness index in relation to speed. According to figure 4.15, when compared to previously published works like HFWOA-VANET, BWO-VANET, and HHO-VANET based on Speed, the proposed approach, H-HHBW-VANET, has a high value of the fairness index.

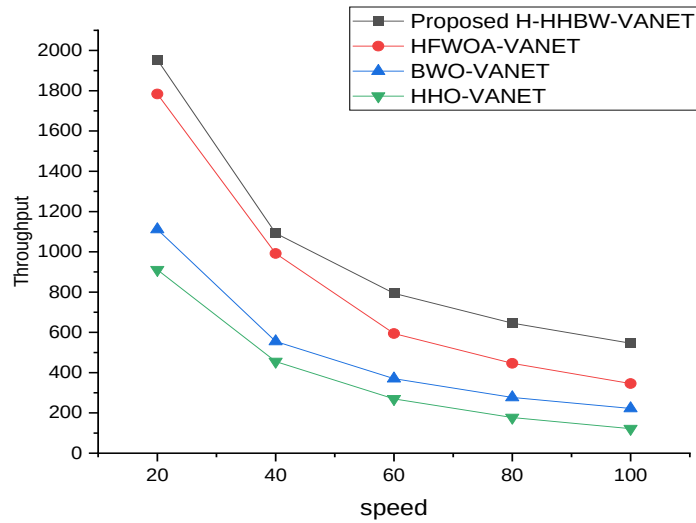


Figure 4.14: The graphical representation of Speed Vs Throughput

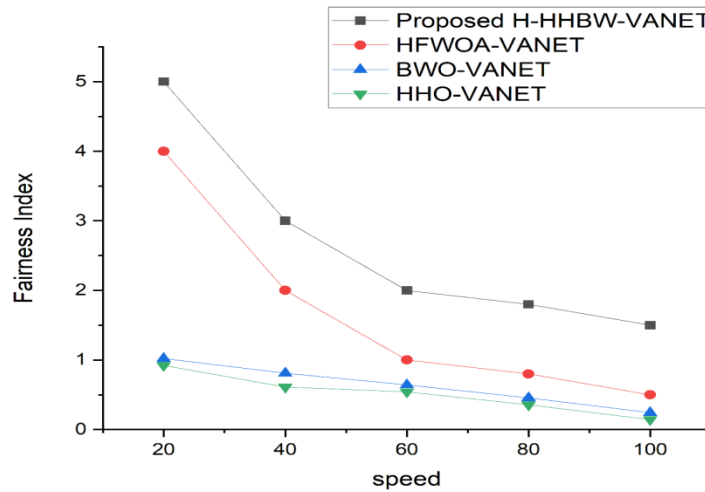


Figure 4.15: The graphical representation of Speed Vs Fairness Index

The suggested strategy is shown to be a more effective way to provide the congestion-free routing process for a dynamic VANET environment by the graphical representation and table of the comparison study of the proposed H-HHBW-VANET with current HFWOA-VANET, BWO-VANET and HHO-VANET.

4.7. Summary

Traffic congestion can be easily detected by VANETs, but simply detecting it is insufficient because there are two types of congestion: recurrent and non-recurrent. The QoS quality analysis and traffic shaping both play a significant part in the routing process. We have put out a methodology that ensures QoS measurements during the congestion-free routing procedure. The suggested system improved QoS for routing between nodes using the Hybrid-Harris Hawks Black Widow optimization-based VANET (H-HHBW-VANET) method. The system was put into place on NS2's operational platform and its effects on QoS performance parameters like Drop, Delay, Energy Consumption, Throughput, and Fairness Index were studied. Two situations, such as node and speed fluctuations, show that the analysis findings are effective. It may be shown that the suggested strategy performs better than existing techniques such, Hybrid Firefly Whale Optimization Algorithm based VANET (HFWOA-VANET), Black Widow Optimization based VANET (BWO-VANET), and Harris Hawks Optimization based VANET (HHO-VANET) for the variation of node and speed. According to the analytical model, the system is effective at directing traffic between nodes for higher throughput and less energy use. As a result, the suggested transport protocol increases QoS performance while being free of congestion.

CHAPTER 5

A ROBUST COMMUNICATION WITH HYBRID TECHNIQUE IN VANET

Vehicular Ad hoc Network (VANET) is one of the popular and promising technologies in the modern intelligent transportation. However, VANET is exposed to several vulnerabilities and leads to intrusion. This intrusion must be solved before adopting the VANET technology. The efficacy of the VANET is therefore enabled by a revolutionary machine learning technique. The suggested approach includes two phases. Phase I detects the DDoS attack using a novel machine learning technique called SVM-HHO, which provides the information about the vehicle. Phase II mitigates the impact of DDoS attack as well as allocate bandwidth using a Reliable Resources Management technique based on Hybrid Whale Dragonfly Optimization Algorithm (H-WDFOA). This proposed model can be considered as an effective technique to predict and utilize the reliable information that provides effective result in smart vehicle. The novel machine learning based technique is implemented through MATLAB platform and in NS2 platform.

5.1. Introduction

In recent years, the importance of the VANET in the networking sector has increased. It is a specific sort of mobile ad hoc network (MANET) that is mostly utilized for vehicle-to-vehicle and vehicle-to-equipment communication. It distributes information through communications between vehicles (V2V), infrastructure (V2I), and everything (V2X). VANET is applicable for various regions such as traffic control, traffic congestion monitoring, and driver safety program. However, VANET has its demerits like dynamic behaviour. This issue is rectified by an effective and efficient routing protocol that broadcasts the data. Because cars might not be able to exchange information and lose all the benefits provided by cutting-edge VANETs technology in the absence of an effective routing plan [271]. Many efforts have been made recently to adapt software-defined network (SDN) concepts to automotive networks in order to benefit from the SDN's features like flexibility and programmability. The ultimate objective of this adaption is to improve the

VANETs' performance and also make them more suited to serve certain services and applications. The software-defined network (SDN) is one of the emerging revolutionary network concepts, utilized in data centres and operator networks to satisfy the growing demands of future networks. Network programmability, centralized management control and interface openness are some of the features of SDN. It also substantially simplifies the network administration and improves networkability [272]. There are three layers in SDN that are data, control and application layer. The data layer includes equipment such as routers, switches, automobiles and wireless devices. According to the controller, which is the brain of SDN and is situated in the control layer, the devices in the data layer are responsible for packet transmission. It controls the flow of data and how data layer devices communicate data. The software used to programme the network is found at the application layer. Despite all the advantages and high performance of SDN and VANET technologies, it has been subjected to attack risks namely DoS and DDoS, just like traditional wireless networks. However, SDN's features make it simpler to identify and respond to DoS attacks. The openness of the data plane creates favorable conditions for additional DoS attacks. Distributed DoS (DDoS) attacks are those that involve several vehicles that are dispersed throughout the network. Due to this intrusion, the targeted system is unable to handle any of the incoming requests and the entire system crashes. In such attacks, the hacker hacks thousands of hosts that include PCs, servers and IoT devices and then exploits them all at once to overload the victim's resources with a significant quantity of traffic. This traffic suspending network users and defending against it is quite difficult. However, a system administrator can detect a potential threat but it could not handle the simultaneous attack in real-time. Therefore, certain security restrictions must be imposed on the SDN controller. Additionally, automatic attack detection systems are required to ensure an optimum level of service quality and to detect suspicious intrusions.

The detection of DDoS attacks includes various challenges that are identifying the characteristics of attack traffic; a lack of cooperation among the nodes of a coherent network; modification in attack tools; usage of fake IP address; and short attack duration and limited response time. To address these problems, a framework is required that identify

the intrusions and store information in communication while maintaining data integrity. The ultimate purpose of the intrusion detection system is to stop attacks as close to their source as possible and to identify infiltration before harm is done to a targeted server. Machine learning (ML) techniques provide such a framework which is frequently employed in VANETs to evaluate large amounts of data and generate efficient rules for attack detection, classification and prediction. The ML approaches are not only applicable to intrusion detection but also in various fields like speech recognition, recommendation systems, medical diagnosis and traffic prediction. It also provides a desirable solution to detect intrusions in advance with acceptable speed and accuracy in VANETs. VANET communication types can be divided into four categories.

- *In-vehicle communications* the term used to describe the in-vehicle domain, which is becoming more and more important and vital in the study of VANETs. An in-vehicle communication system, which is crucial for both driver and public safety, may identify a vehicle's performance, notably the driver's level of fatigue and exhaustion.
- *Vehicle-to-vehicle (V2V) communication* can offer a data exchange platform so that drivers can share knowledge and alerts to increase driver assistance.
- *Vehicle-to-road infrastructure (V2I) communication* is another fruitful area for VANET research. Real-time traffic and weather updates for drivers are made possible via V2I communication, which also offers environmental sensing and monitoring.
- *Vehicle-to-broadband cloud (V2B) communication* suggests that 3G and 4G wireless broadband technology may be used by automobiles for communication. Because the broadband cloud may have more traffic information and monitoring data in addition to infotainment, this type of connectivity will be beneficial for active driver assistance and vehicle tracking.

5.2. Improved Machine Learning in Robust Communication

The VANET's dynamic condition is developed in this section to select the suitable routing of each node. Furthermore, allocating the bandwidth of each node is obtained for an accurate routing. To provide an accurate bandwidth allocation for proper routing process in a VANET scenario, the optimization approach SVM-HHO-VANET is developed to select route based on clustering. Here, the proposed methodology is halved into two phases. Security-based Modified SVM is utilized to detect DDoS attack in the initial phase. Finally, in the next phase, the HHO optimization approach for the VANET dynamic scenario is helped to achieve the effective bandwidth allocation. With vehicle QoS parameters, cluster selection, accurate cluster nodes communication, detecting DDoS attack, route prediction and allocation of bandwidth between the cluster nodes can be achieved effectively. Distance, velocity, speed, bandwidth, number of nearby vehicles and throughput are taken as the parameter of vehicles in this work. Additionally, the evaluation metrics like energy consumption, delay, and drop is considered for analysis of QoS performance.

5.3 Background of HHO, SVM, DDoS attack

5.3.1 Harris hawk's optimization (HHO)

Swarm-based optimization is done using Harris Hawk's Optimizer (HHO). The basic goal of HHO is to imitate the natural hunting behaviour of the Hawk team and the prey's flight in order to find solutions to the single-objective problem. In HHO, the best location is represented by the prey, while the hawks' chasing behaviours reflect the search agent. HHO can be extremely helpful in resolving many optimization issues that arise in the real world (e.g., problems with power quality, geotechnical engineering, pattern recognition, manufacturing optimization, feature selection, image segmentation, and medication design are all examples of engineering design and optimization issues). The HHO can also be used to handle issues involving discrete and continuous spaces, as well as problems with unknown types of search space. It offers greater solution quality, high accuracy in extracting the optimal parameter, and improved prediction performance. Additionally, it was

confirmed that HHO is a potentially strong optimizer that aids in the faster and more straightforward computing of the best solution to difficult nonlinear problems.

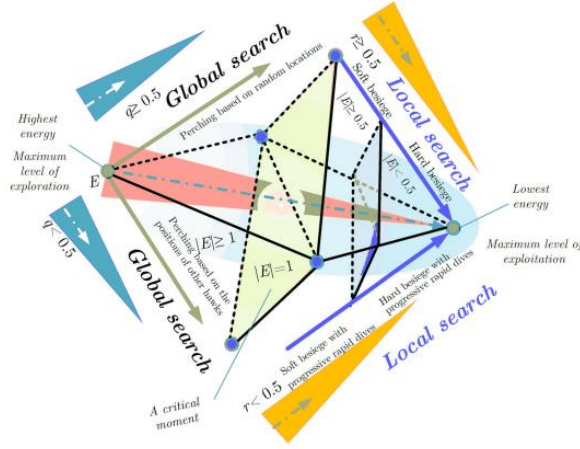


Fig5.1: A widespread demonstration of the phases of the HHO

Fig 5.1 explains the demonstration of the HHO and the explanation of phases of HHO are detailed below.

5.3.1.1. Exploration phase

This stage explains the hawk's location while scouting out its prey. It is reliant on two different strategies. The first method describes how hawks locate prey based on where the actual members are $(T(it), it = 1, 2, 3, 4, \dots, N)$ (where N represents the number of hawks, and Eq (5.1)). The second method, however, describes how hawks find prey in accordance with where they sit in a random tree T_{RD} , which is modeled in eq. (5.1)

$$T(ITER + 1) = \begin{cases} T_{RD}(it) - Ri_1 |T_{RD}(it) - 2Ri_2 T(it)| & I \geq 0.5 \text{ rule} \\ ((T_{RAB})(it) - t_m(it)) - Ri_3 (Lp_{bound} + R_4 (Up_{bound} - Lp_{bound})) & I \geq 0 \text{ rule} \end{cases} \quad (5.1)$$

Where,

$$T(ITER + 1) \Rightarrow \text{The position of Hawks will be in the next iteration (it)}$$

it $\Rightarrow$ Iteration,

T_{RAB} $\Rightarrow$ Prey's Position

$T_{RD}(it)$ $\Rightarrow$ Current population-based random solution selection
process

$T(it)$ $\Rightarrow$ Position of the Hawks in the current position "it",

Ri_1, Ri_2, Ri_3, Ri_4 , and I $\Rightarrow$ The range between [0,1] and the random scaled factor is updated in each iteration.

Lp_{bound} $\Rightarrow$ Variable of a lower bound.

Up_{bound} $\Rightarrow$ Variable of upper bound.

t_m $\Rightarrow$ Average no of solutions.

These two strategies are used in combination with the (Lp_{bound} - Up_{bound}) targeting method, which facilitates in identifying the hawks' position. These strategies can be described by two points such as (I) Other hawks are generating the random answer based on present population., and (II) The model is generated using the hawk's average position, prey location and random scaling factors. The value of Ri_4 is almost there to 1 when Ri_3 is considered as a scaling factor. The unpredictability rule can be improved using these actions. The length of the randomly adjusted moment is integrated into the LB. The random scaled features offer the diversification strategy, and the different aspects of the feature space are then examined. The average position of responses is calculated using the equation.

$$t_m(ite) = \frac{1}{N} \sum_{i=1}^{TOTAL} T_i(it) \quad (5.2)$$

where,

$t_m(ite)$ $\Rightarrow$ The average solutions in the current iteration-based coordinates.

$TOTAL$ $\Rightarrow$ Total possible solutions.

$T_i(it)$ $\Rightarrow$ Each solution-based location is based on iteration it .

During the capture of prey, the hawks do random solution procedures.

5.3.1.2. Exploitation phase

The primary two components of this phase are hawk chasing tactics and prey fleeing behaviours. The purpose of this phase is to simulate the surprise pounce (seven kills) behaviour of hawks on the investigated prey. Four chasing techniques are given to achieve this: (1) hard besiege; (2) soft besiege; (3) hard besiege with progressive fast dives; and (4) soft besiege with progressive rapid dives.

5.3.2. Support Vector Machine (SVM)

Support Vector Machine (SVM) has developed into a productive classification paradigm. The strongest classification and regression mathematical model is SVM. This strong mathematical underpinning provides a fresh angle for further investigation into the large topic of classification and regression. SVM has undergone numerous improvements over the past few decades, Lagrangian SVM, including twin SVM, Least Square Support Vector Machine, Quantum Support Vector Machine, etc. SVM is gaining popularity because it has a solid mathematical foundation and appears to work reasonably well in a variety of different real-world applications. Inspiration from their improved image and data mining categorization accuracy. SVM is a supervised learning method used in the fields of classification and regression. It is highly effective and has a strong statistical basis. Numerous modifications to SVM have been developed over the years, including Twin SVM, Least Square SVM, Lagrangian SVM, DAG SVM, Decision Tree SVM and multi kernel classification. The two most common methods used by SVM to convert multi-class classification into multiple binary classifications are OvR (One Vs Rest) and OvO (One Vs One).

Binary classifiers are needed by OvO for the N-class classification problem. OvR uses a single classifier for each class, treating the dataset for that class as positive data and

the rest as negative data. OvR implements a succession of binary classifiers, each of which distinguishes one class from the others, for this kind of comparison. For each test set of data, OvR requires N binary comparisons. OvR has a lower computational complexity than OvO. By converting the initial training data into multidimensional space and SVM conducts classification, creating hyper-planes in higher dimensions. SVM is a mathematical learning strategy based on optimal hyper-planes. Through the creation of a hyper-plane in higher dimensions, an SVM conducts classification. This hyper-plane corresponds to the decision planes in Fig. 5.2, which are used to distinguish between groups of data of different types. A data set is always categorized by the creation of a hyper-plane in an appropriate nonlinear mapping for higher dimensional space. The support vector method (SVM) looks for those vector points that form the decision border and provide a significant marginal separation between the classes. In the decision plane, SVM distinguishes the classes with the greatest marginal distance. The middle line shows the hyperplane with the highest margin. In other words, one would select a boundary line that separates the two classes and is located the greatest distance from the closest data point. Vapnik's theory defines the decision boundary or hyper-plane for classification for the two class problem.

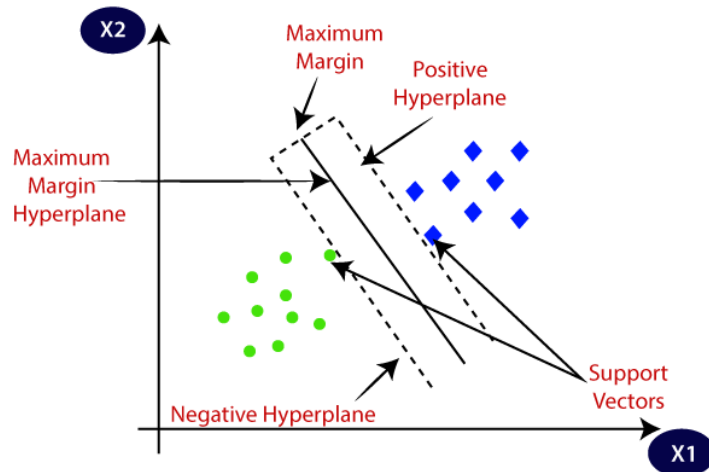


Fig 5.2:hyperplane supporter in SVM plane

If input set is X_i is $m * n$ dimension and corresponding class is $Y_i \in \{-1, +1\}$.

$$W^T \phi(X_i) + b = 0 \quad (5.3)$$

The hyperplane is designed to satisfy the inequality function for both classes, which is shown below.

$$W^T \phi(X_i) + b \geq +1 \quad y = +1 \quad (5.4)$$

$$W^T \phi(X_i) + b < +1 \quad y = -1 \quad (5.5)$$

$$y_i(W^T \phi(X_i) + b) \geq +1 \quad i = 1, 2, 3, 4 \dots N \quad (5.6)$$

5.3.3. Distributed denial of service (DDoS) attack

A threat to network security known as a distributed denial of service (DDoS) attack seeks to overwhelm the target networks with malicious traffic. Even though there are numerous statistical techniques for detecting DDoS attacks, creating a real-time detector with little processing overhead remains one of the key challenges. On the other hand, the evaluation of novel detection algorithms and methods strongly depends on the availability of datasets that have been well planned. An extremely effective method of attacking intranet and internet resources is a (DDoS) attack. A significant number of hacked devices typically prevent normal users from using web-based services in this assault. DDoS assaults can be carried out via a variety of protocols, including TCP, UDP, ICMP, and HTTP, at the network, transport, and application layers. In the last few years, distributed denial-of-service (DDoS) assaults have received a lot of attention online. The principles and methods of Software Defined Networking (SDN) have been introduced and extensively studied in recent years. Due to the SDN network's different architecture from traditional networks, DDoS assaults may pose a threat to its availability. The SDN controller in particular is the component most susceptible to DDoS attacks. The goal of a DoS attack is to block legitimate users from accessing a network's resources. One such major threat in the cloud environment is DDoS. In this work, we report new breakthroughs in cloud-based DDoS attack mitigation techniques. We give a thorough analysis that provides a thorough understanding of the characterization, prevention, detection, and mitigation mechanisms of

these attacks. We also provide thorough solution taxonomy to categorize DDoS attack remedies. We also offer a thorough analysis of key indicators for comparing alternative solutions. This study finds a significant need for solutions that are created with utility computing models in mind. Some of the primary needs of the required solutions are defence leveraging extensive cloud resources, multi-layer mitigation, and accurate auto-scaling judgments. We conclude by offering a clear framework for developing effective solutions and comprehensive solution specifications to assist the cyber security research community in developing protection mechanisms.

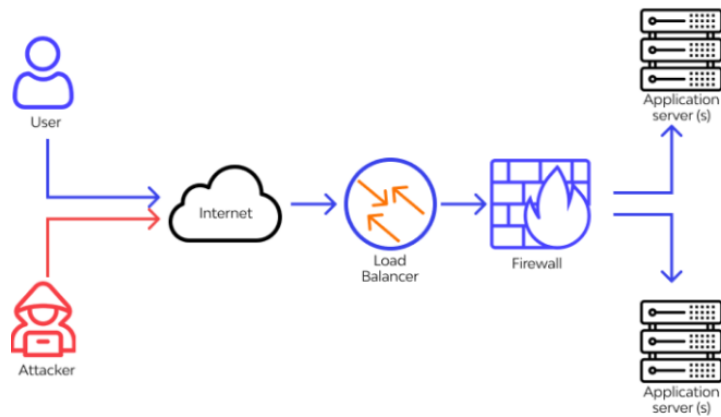


Figure 5.3:DDoS attack

5.3.3.1.Types of DDoS attacks

➤ Application layer attacks

Application layer attacks, which include DoS and DDoS risks, aim to overwhelm a server by delivering numerous requests that must be handled and processed with a lot of resources. Among the attack techniques in this category are HTTP floods, slow attacks (such as Slowloris or RUDY), and DNS query flood attacks. Requests per second (RPS) are a popular unit of measurement for the intensity of application layer attacks, with the majority of medium-sized websites typically just requiring 50 to 100 RPS to become useless.

➤ **Network layer attacks**

DDoS attacks targeting your network's "pipelines" are usually always network layer attacks. This category of attack methods includes NTP amplification, DNS amplification, NTP flood, SYN flood, and other types of attacks. Any one of these can be exploited to block access to your servers and result in serious operational harm like account suspension and exorbitant overage fees. DDoS assaults are frequently high-traffic occurrences with common measurements in gigabits per second (Gbps) or packets per second (PPS). Although the majority of network infrastructures can be completely destroyed with 20 to 40 Gbps, the most potent network layer attacks can reach hundreds of Gbps.

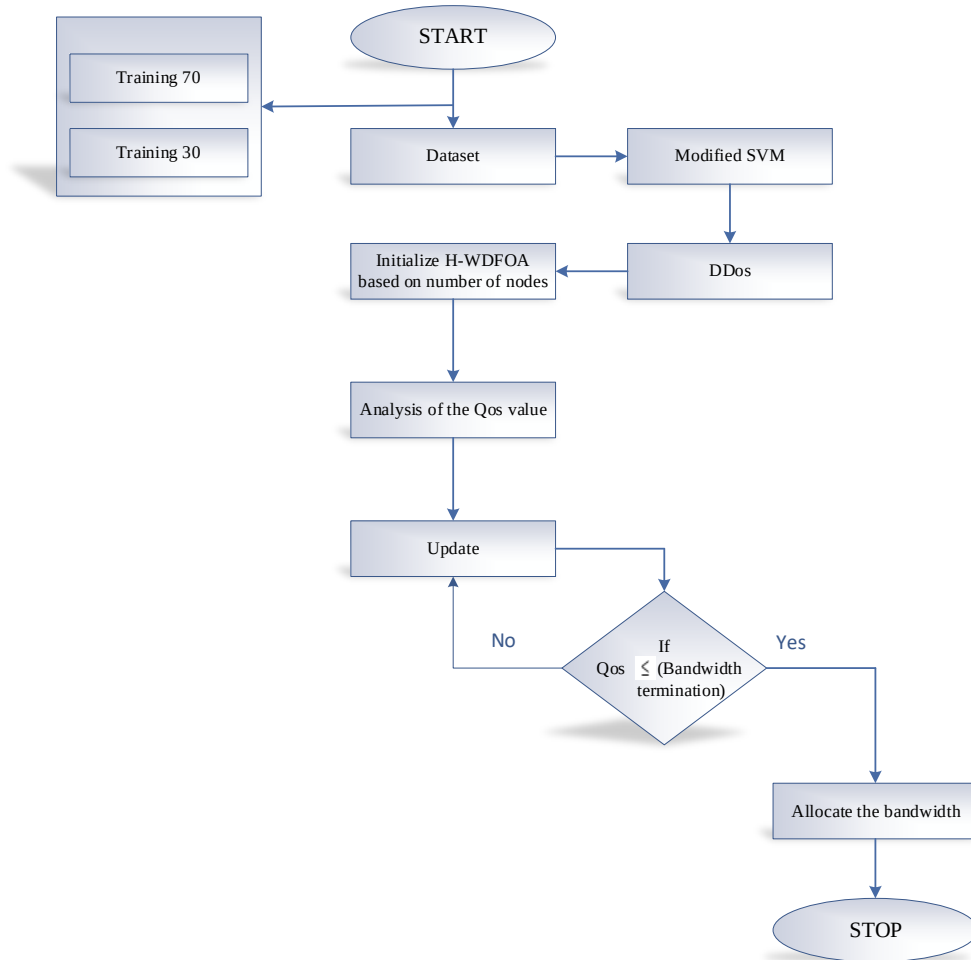


Figure: 5.4Flowchart for Proposed Methodology

The flowchart of proposed methodology is illustrated in Figure: 5.4. Initialize the dataset, where 70% of data are utilized in training phase and 30% of data are used in the testing phase. However, DDoS attack is analyzed and detected by Modified SVM. Due to DDoS attack, the performance of node is reduced, and bandwidth attract more attenuation. In addition, based on number of nodes Hybrid WDFOA is initialized for allocating bandwidth. For allocation, QoS value is analyzed separately based on bandwidth, distance, speed, velocity of the vehicle. The capacity of node to transfer node is determined by executing condition evaluation, if the bandwidth of node is less. To enhance the bandwidth the DF optimization is integrated with WOA. Condition is repeated until the termination of bandwidth is allocated.

5.3.4 Simulated VANET

Users benefit via VANET's services like reduced traffic congestion, convenience, entertainment and enhanced road safety. Mobile ad hoc network (MANET) resembles a VANET. Although, the rapid speed of the vehicles is a distinct feature. The VANET is derived from the Intelligent Transportation System (ITS) and the Wireless Access Vehicle Environment (WAVE). A Global Positioning System (GPS), sensors, wireless access protocols and entertainment networks are assembled the VANET. The surrounding environment and its content are sensed by a vehicle. In order to avoid collision, sensors are utilized to predict objects ahead (ex. Front automobiles) and obstacles. It also employs onboard wireless communication to provide users with real-time information on road conditions, like traffic entertainment and other social apps.

At fixed location, utilizing 1000 vehicles, VANET has been implemented randomly and placed in area 1000*1000 m. The placement of vehicles is tabulated in Table: 5.1. In a defined area, VANET have placed randomly.

Table 5.1: Vehicle placement in the VANET

At random places, vehicles are places to create VANET
➤ In Total – Vehicles, For each x ➤ $Va(x) = 1000 * \text{run if } (1)$ ➤ $Vb(x) = 1000 * \text{run if } (1)$ ➤ $Fix (V a(x), V b(x))$ ➤ End For

The a and b are the coordinator of the vehicle, denoted by Va and Vb . To place a vehicle in random position at location a and b, R-studio is utilized to in-build random function run if (1).

5.3.5 Dataset Production

Researchers utilize machine learning and deep learning research dataset i.e., “DDoS attack-based SDN Dataset”, which is available in SDN environment and access publicly in this work. The dataset, which contains 104345 traffic, flows in 23 features. The normal and attack traffic class label uses dataset consists of UDP, ICMP, and TCP traffic.

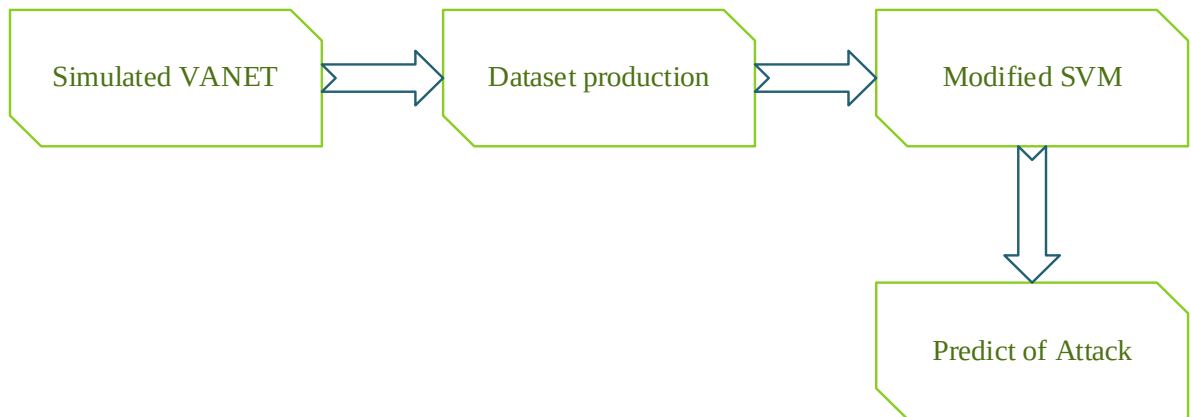


Figure5.5: Basic Architecture for Detection Method

5.4 Phase: 1 – Security-based Modified SVM

The Modified Support Vector Machine (MSVM) is utilized in this research to detect DDoS attacks on SDN-based VANETs. A binary classification problem is a classification problem of DDoS detection. The two types of DDoS detection are Normal or DDoS attack. In VANET, the DDoS detection problem need swiftness and very high accuracy owing to its highly critical essentials. For classification, a wide range of approaches are designed, such as K-NN, ANN, SVM, Deep Learning-based CNN, but the SVM, which is based on machine learning, was most demanding and robust classifier in solving this difficulty. Here, to a high-dimensional space, SVM utilizes kernel function to transfer non-linear data based on Harris Hawks Optimization (HHO). In the SVM classifier, optimal kernel is selected based on HHO is known as Modified SVM. So, the kernels-based MSVM are proposed in this work to detect DDoS attacks.

This section discusses the hybrid detection method based on the MSVM kernel. Figure 5.5 depicts the architecture of the suggested hybrid detection. The system's three modules are VANET simulation, dataset production and the proposed hybrid approach. The VANET setup consists of 1000 vehicles in the first module. For creating training and testing process, the second module generates the required data. Finally, to generate predictions, the training and testing process is fed to hybrid technique. For indicating efficient behavior or DDoS attack, prediction consists of binary value “0 or 1”.

Here, a Support Vector Machine (SVM) is an extension of SVC that utilizes various kernels-based on HHO to expand the feature space. A MSVM may work on non-linear classifications by employing kernels. Two similar interpretations determine the kernel function. Input data is converted into desired form by using kernel function. In this work MSVM is utilized to predict DDoS attack. The back ground details of MSVM are discussed below:

5.4.1 Modified Support Vector Machine (SVM)

For classification problems, it was claimed as best method. Maximal margin classifier is the generalized version of SVM. Margin is the name for the shortest distance between an observation and a hyperplane. A flat affine subspace in an x-dimensional space gives rise to a hyperplane's x-1 dimension [273]. The given equation defines a 2 dimension in a hyperplane.

$$\alpha_0 + \alpha_1 y_1 + \alpha_2 y_2 = 0 \quad (5.7)$$

Here, in hyperplane $Y = (Y_1, Y_2)^T$ is a point and α_0, α_1 and α_2 are the parameters. Equation (1) can be extended, for n-dimensional space.

$$\alpha_0 + \alpha_1 y_1 + \alpha_2 y_2 + \dots + \alpha_n y_n = 0 \quad (5.8)$$

If $Y = (Y_1, Y_2, \dots, Y_n)^T$, Y lie on hyperplane.

If x is higher than zero, it is on one side of the hyperplane; otherwise, it is on the other. This is based on the left-hand side of Equation (5.8) being greater than zero. In this way, a hyperplane tells which side a point is on.

A 2-dimensional space's solid line for the maximal margin hyperplane. The probability of the observation that is closest to the maximal margin hyperplane is shown by dotted lines. Margin is the line that joins one of the dotted lines to the solid line. It is indicated by an arrow. A technique makes the decisions that result in the circles and stars.

The margin is largest, when the hyperplane is separated from the maximal margin hyperplane. The maximal margin classifier approach that classifies test observations based on side of the hyperplane lies. However, the classification can be overfit due to single change in observation and it is overly sensitive.

A Support Vector Classifier (SVC) permits certain observations to be misclassified, resulting in some observations being on the wrong side of the margin. As a result, this

classifier is sometimes referred to as a soft margin classifier. Based on which side of the hyperplane a test observation is located, the SVC can categorize it. Observations regarding Figure 5.6: are outside the limits of the hyperplane.

The equation expressed the SVM's working principle,

$$\text{Maximize}_{\alpha_0, \alpha_1, \dots, \alpha_n, \epsilon_1, \dots, \epsilon_n} \quad (5.9)$$

A circumstance,

$$\sum_{i=1}^n \alpha_i^2 = 1 \quad (5.10)$$

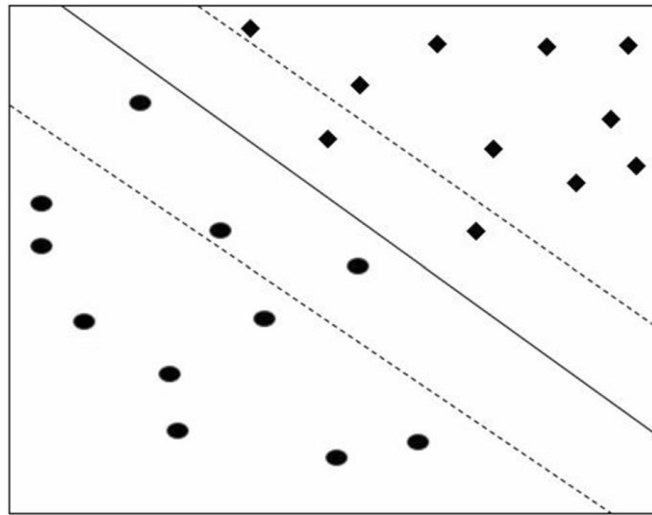


Figure 5.6: Concept of Support Vector Machine (SVM)

$$f_x(\alpha_0 + \alpha_1 y_1 + \alpha_2 y_2 \dots \dots + \alpha_n y_n) \geq W(1 - \epsilon_x) \quad (5.11)$$

$$\epsilon_x \geq 0, \sum_{x=1}^n \epsilon_x \leq T \quad (5.12)$$

In this case, positive tuning parameter is denoted by T . The width of the margin is represented by W . A slack variable is ϵ_x , which allows an observation on the wrong side of the margin. The sign of $\alpha_0 + \alpha_1 y_1 + \alpha_2 y_2 \dots \dots + \alpha_n y_n$ is classified as observation.

Now, to transfer non-linear data, SVM uses kernel function-based on HHO, known as MSVM. To detect DDoS attack, MSVM is employed. Hence, the optimal kernel-HHO is detailed as follows:

5.4.2. Selection of Optimal Kernel based on Harris Hawks Optimization (HHO)

Harris Hawks Optimization (HHO) is population-based meta-heuristic approach inspired by nature. Harris Hawk's cooperative hunting behaviour for prey such as rabbits. Exploration, Transformation and Exploitation are the three steps included in the HHO optimization technique.

5.4.2.1. Initialization Phase

The initial hawk's population was initialized as the solution for this phase. The number of nearest vehicles ($n_1, n_2, \dots, n_N$) encompasses the population. Here, number of populations are denoted as N . The execution of the technique was done by cluster vehicle (n_{cl}). The cluster as well as nearby vehicles are denoted as "hawks", while the destination vehicle is referred as prey (rabbit). For all vehicles, the fitness function is determined in this phase. The fitness of j^{th} vehicle is calculated as follows,

$$f(n_j) = \{\sum D, M, \delta, K\} \quad (5.13)$$

Here, the fitness function is developed as mobility (M), direction (D), vehicle state (δ), and available of spectrum (K). Binary values '0' and '1' are described as direction of vehicles. The fitness of the vehicle will be enhanced, if target and cluster vehicles are in same direction, then $D = 1$ or 0. Furthermore, to enrich the computation fitness, the mobility will be mapped as 0 and 1. When $M = 0$ or 1, mobility of n_j is higher than average mobility. For data transmission $K = 0$ or 1, if n_j has available channel. The function of evaluation metrics is represented as follows:

$$\delta = \frac{P+DR}{D} \quad (5.14)$$

The throughput function of δ is n_j (P) for n_j , delay (D), and data rate (DR). For data transmission, optimal path can be achieved by deciding factor δ of computation fitness with effective channel estimation. In the population, for all vehicles, $f(n_j)$ is computed.

Exploration, transformation and exploitation are the three phases of HHO. To observe and catch rabbit, Hawks found different locations randomly during exploration phase. At the exploration phase, the hawks exploit the presence of nearby vehicles. As cluster solution, Hawks positions are regarded. For rabbit, the best position is expected. Three phases are describing as follows:

5.4.2.2.Exploration Phase

During this phase, the waiting, searching, and prey detection processes are carried out. The following illustrates how a hawk would argue,

$$n_j(V+1) = \begin{cases} n_{j_{rand}}(V) - \gamma_1 |n_{j_{rand}}(V) - 2n_j\gamma_2 \\ (V)| \text{ if } m \geq 0.5 \\ n_{j_q}(V)n_{j_a}(V) - \gamma_3(l_1 + \gamma_4 \\ (v_b - l_1)) \text{ if } m < 0.5 \end{cases} \quad (5.15)$$

The current iteration is denoted as V , while the following iteration is denoted as $V + 1$. Hawk locations are denoted by γ_1 , γ_2 , γ_3 and γ_4 , while the random integer y was expressed by the interval $[0, 1]$. The average hawk location, $n(j(a))$, is written as,

$$n_{j_a}(V) = \frac{1}{N} \sum_{i=1}^N n_j(V) \quad (5.16)$$

5.4.2.3.Transformation Phase

The exploitation phase sees a shift from the discovery phase. Prey energy was broken down as the prey was evading. This was specified as,

$$\omega_{prey} = 2\omega_0 \left(1 - \frac{V}{V_{max}}\right) \quad (5.17)$$

Where, the current iteration is indicated as V , the maximum iteration number is represented as V_{max} , and the initial energy state of the prey is ω_0 .

5.4.2.4. Exploitation Phase

The hawk's attack on the selected prey in the initial phase is used to assess it. These four diverse tactics—soft besiege, hard besiege, soft besiege with progressive fast dives, and hard besiege with progressive fast dives—are being assessed in this phase. In terms of energy level, the frequency of hard and soft relies were $|\omega_{prey}| \geq 0.5$ and $|\omega_{prey}| < 0.5$.

Besiege for Soft:

If $|\omega_{prey}| \geq 0.5$ and $\gamma \geq 0.5$, the soft besiege method can be chosen. It's described as,

$$n_j(V + 1) = \Delta n_j(V) - \omega_{prey} |\zeta n_j(V - n_j(V))| \quad (5.18)$$

Here, the method of dodging the leap intensity ζ is based on $\zeta = 2(1 - \gamma_5)$ and $\Delta n_j(V) = n_{prey}(V) - n_j(V)$.

Besiege for Hard:

If $\gamma \geq 0.5$ and $|\omega_{prey}| < 0.5$ the hard besiege method can be chosen, it is outlined as:

$$n_j(V + 1) = n_{prey}(V) - \omega_{prey} |\Delta n_j(V)| \quad (5.19)$$

Besiege for Soft with High Progressive Dives:

If $\gamma < 0.5$ and $|\omega_{prey}| \geq 0.5$, the soft besiege method can be chosen. It is established that:

$$Q = n_j(M) - \omega_{prey} |\zeta n_{prey}(V - n_j(V))| \quad (5.20)$$

The hawk's subsequent movement is calculated (ϱ). Additionally, when hawks dive, the following equation is expressed to attack the prey:

$$D_n = \varrho + R * LF(d) \quad (5.21)$$

Where the dimension d of levy flight is defined as $LF(d)$ and the random vector is written as R . The newly discovered locality is identified as,

$$n_j(V+1) = \begin{cases} \varrho & \text{if } f(\varrho) < f(n_j(V)) \\ D_n & \text{if } f(D_n) < f(n_j(V)) \end{cases} \quad (5.22)$$

Besiege for Hard with High Progressive Dives:

Soft besiege method has been selected, if $\gamma < 0.5$ and $|\omega_{prey}| < 0.5$. It is determined by the updated location:

$$n_j(V+1) = \begin{cases} \varrho & \text{if } f(\varrho) < f(n_j(V)) \\ D_n & \text{if } f(D_n) < f(n_j(V)) \end{cases} \quad (5.23)$$

From, the following equation is determined by ϱ ,

$$\varrho = y_{prey}(V) - \omega_{prey} || \zeta n_{prey}(V - n_{ja}(V)) || \quad (5.24)$$

The population based on fitness is updated the location of prey, based the way of HHO approach. Thus, the detection of DDoS attack is classified effectively by utilizing MSVM.

5.5 Phase: 2- Reliable Resource Management using H-WDFOA-VANET

Hybrid Whale-Dragonfly Optimization-based VANET (H-WDFOA-VANET) reliable resource management is utilized to allocation of bandwidth in this work. The proposed H-WDOA approach is explained and then the background of WOA and DF optimization techniques is discussed individually. In a dynamic VANET scenario, a combination of Whale and Dragonfly Optimization Algorithm is represented as H-WDFOA.

To achieve bandwidth allocation and to obtain routing of the vehicle, the H-WDFOA is employed. To obtain the designation path, latency and bandwidth utilization are also initiated by protocol routing. It is difficult for safety-related and critical time. So, in order to overcome this problem, the efficient H-WDFOA technique is utilized to allocate bandwidth and routing protocol, also this allocation technique is explained in the following section.

5.5.1 Hybrid WDFOA-VANET

The suggested methodology couples the meta-heuristic-based WOA and DF methodologies to study the influence of QoS value in the dynamic VANET environment.

The hunting behavior of humpback whales are considered for the generation of whale Optimization Algorithm (WOA). For executing the bubble-net feeding procedure, a tiny fish and krills are taken as a whale's prey. For confusing their prey, the whale moves 12 m downwards or made 9 shaped spiral bubbles to execute. For hunting prey, they reach sea's surface. For encircling and bubble net approach, two whales are involved. In this work, vehicles are considered instead of whales. To get more details, systematic techniques are explained below.

5.5.2 Encircling Prey Method

The current best method, for the humpback whale to examine the location of its prey and encircle them, while WOA assumes its prey as target. The best search agent is considered after examining the present best solution. Similarly, by increasing maximum iteration, additional search agents can modify their positions in order to approach the best search agent. The vehicle's parameters, including distance, speed, velocity, the number of nearby vehicles and throughput, are used as the initial population during the initialization phase. The mathematical version of this operation is represented by the equation below.

$$M = |V \cdot P^*(t) - X(t)| \quad (5.25)$$

$$P(t + 1) = P^*(t) - B \cdot M \quad (5.26)$$

Where,

$t \rightarrow$ Present Iteration,

B and $V \rightarrow$ Coefficient Vectors,

$P^* \rightarrow$ Obtained best solution's position vector.

$P \rightarrow$ Position Vector

On determining the best solution, P^* every iteration is updated periodically in this process,

$$B = 2x * r - x \quad (5.27)$$

$$V = 2 \cdot x \quad (5.28)$$

Here, $r \rightarrow$ random number which range from 0, 1.

Variable's range is reduced from 2 to 0 in exploitation and exploration phases. To fetch optimized solution, global search process is executed by exploitation phase. By executing big jumps, local search is taken in exploitation to search space. Effective outcomes can be achieved successfully.

5.5.3 Technique for Bubble-net Attacking

Spiral updating and shrinking encircling are the two progresses of attacking whale's significant step for bubble-net method. The shrinking encircling and spiral updating processes re described as follows.

5.5.4 Mechanism for Encircling Shrink

In the course of iteration, a significant variable will reduce from 2 to 0. At the interval $[-1,1]$, the phase shown major difference. It is possible for a vehicle to move from its initial position to a new one. In 2D space of interval $[-1,1]$, X and Y to X^* and Y^* are the possible position achieved.

5.5.5 Prey Search

From the exploitation phase, to find prey the random searching process is executed by humpback whales. The variation of the vector is determined by this phase. To the current best individual, the updating position is executed if $|A| < 1$ taken place in exploitation condition. Conversely, to choose individual for the global optimum $|A| > 1$ comes the exploration process is executing in random selection. Furthermore, the position is executed by updating the procedure, and mathematically represented as:

$$M = |V \cdot P_{rand} - P| \quad (5.29)$$

$$P(t + 1) = P_{rand} - B \cdot M \quad (5.30)$$

5.5.6. Updating Position for Spiral

To calculate the spiral updating technique can be constructed for analyzing the distance of whale and the prey required. Then the spiral path is determined based on the position of both the whales and its preys in order to execute the movement in terms of helix-shaped by whales. The equation below determines how this procedure works.

$$P(t + 1) = M' \cdot e^{sr} \cdot \cos(2\pi r) + P^*(t) \quad (5.31)$$

Here, M' is the distance of whale $P(t)$ towards prey $P^*(t)$

t is the iteration

indicates a logarithmic spiral's form.

r represents a chance number in the $[-1, 1]$ range.

$$P(t + 1) = \begin{cases} P^*(t) - B \cdot V & \text{if } p < 0.5 \\ M' \cdot e^{sr} \cdot \cos(2\pi r) + P^*(t) & \text{if } p > 0.5 \end{cases} \quad (5.32)$$

To update whale position, 50% probability is chosen for shrinking encircling mechanism or spiral model Here, r denotes random number between the range $[0,1]$.

To getting, maximum optimal solution Dragonfly optimization approach is hybrid with Whale Optimization Algorithm to allocate the bandwidth.

The dragonfly's population is initialized in terms of vehicle nodes of n_j^* .

$$n_j^* = n_1^*, n_2^*, \dots, n_n^* \text{ Here, } j = 1, 2, \dots, n. \quad (5.33)$$

In an inquiry space and development reproduce, the dragonfly's artificial position is updated i.e., position (X) and step (ΔV). The development of dragonfly and characters are demonstrated by progression vector.

$$\Delta X_{t+1} = (wW_i + mA_i + nC_i + pF_i + qE_i) + \varpi \Delta X_t \quad (5.34)$$

Here, weight separation is w , weight aliment is m , weight of cohesion is n , food factor id p , enemy factor is q , inertia weight is ϖ , and count iteration is t .

Position vector can be determined as:

$$X_{t+1} = X_t + \Delta X_{t+1} \quad (5.35)$$

Enhancement phase, various explorative and exploitative process are procedures accomplished. When there is no nearby solution, the dragonfly's situation is updated using Cauchy mutation probability. The position vector X is determined by,

$$X_{t+1} = X_t + N_p X_t \quad (5.36)$$

In the entire swarm at any moment, food source and enemy are determined by entire arrangement. Thus, the accurate vehicle node is selected and the allocation of bandwidth is achieved. A brief flow chart is visualized below.

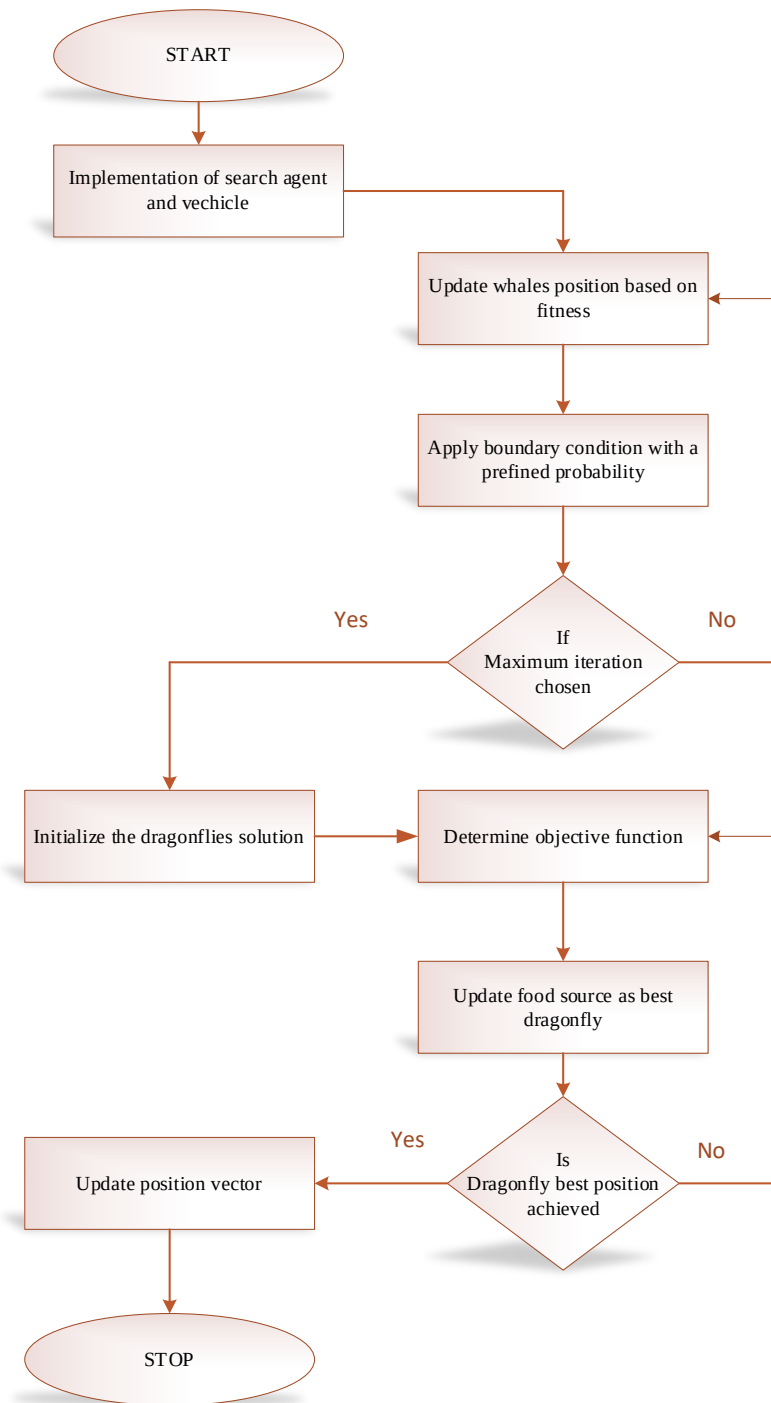


Figure5.7 Flowchart for H-WDFOA-VANET

In the Figure5.7, the flowchart of the hybrid WDFOA-based VANET is visualized. Initially, the Whale optimization parameters are initialized based on search agent. In this work, number of nodes in vehicle are analyzed based on distance, speed, velocity, and bandwidth. The location of vehicle is determined in each iteration according to fitness. When the position of the node is less than 0.5 and nearby vehicle is greater than or equal to 1, update best location. The position of the target vehicle is thought to be the optimal location if the current iteration is higher than the maximum iteration. To achieve maximum optimal solution, the DF approach is integrated with WOA. Furthermore, dragonfly solution is initialized and determines the bandwidth by QoS value according to the objective function. The maximum iteration is utilized until the process is continue and to enhance the bandwidth. Finally, for accurate routing, energy consumption, delay, and drop are considered based on QoS parameter. The proposed approach is accurate in allocating bandwidth, when compared with other existing techniques. This study is robust and fast to predict DDoS attack using MSVM and also to allocate the bandwidth using H-WDFOA technique, in the best position after validation for stability in vehicular networks.

5.6. Results and Discussions

5.6.1. Dataset Description and Evaluation Metrics

The specific SDN dataset is generated using the Mininet emulator useful in traffic classification purposes with the machine and deep learning algorithms [274]. This research starts with ten topologies in the Mininet emulator, in which these switches are interconnected to a single Ryu controller. The network simulators run on ICMP, UDP, and TCP traffic and the malicious traffic are a group of UDP Flood attacks, TCP Sync attacks, and ICMP attacks. The dataset contains a total of 23 features, some of which are obtained from switches and others of which are estimated. Byte count, Switch-id, duration-sec, Packet-count, and duration-nsec are among the retrieved features (Duration in nanoseconds). Summarizing duration-sec and duaration-nsec yields the overall duration. The entire amount of bytes commuted from the switch port is shown by the destination IP, source IP, port number, and the term "tx-bytes." Rx-bytes is the total number of bytes received across the

switch port. The dt field refers to the time and date which is converted into numbers the flow is monitored between 30-second intervals. Moreover, the calculated features such as Packet per-flow and byte per-flow calculate the packet count as a single flow. The total number of packets sent per second, or packet rate, is calculated by dividing the total number of packets delivered each flow. The terms "tx-kbps," "rx-kbps," and "port bandwidth" refer to the data transmission and reception speeds, respectively. The class labels present in the columns refer to whether the type of traffic is malicious or benign. However, Labels 0 and 1 indicate as follows benign & malicious. The duration of the network simulations is 250 minutes and the row of data possessed is 1,04,345. Along with the detailed interval, the simulation of data has been authenticated. For the testing and training processes, the dataset was split into 30% and 70%, respectively. Within 42 seconds, the full training process was finished.

Table 5.2:Simulation Configuration

Parameter	Value
Platform	MATLAB 2020a
Computer	Windows 10 PRO
Processor	Intel ® core (7M) i3-6100CPU @ 3.70 GHz processor
RAM	16 GB

The simulation configuration of the suggested system is described in the table. The suggested platform in this uses MATLAB 2020a and a Windows 10 PRO PC with a total RAM capacity of 10GB and an Intel TM core (7M) i3-6100CPU running at 3.70 GHz as the processor.

5.6.2.Existing Techniques

By combining the concepts of the Rider Optimization Method (ROA) and Cuckoo Search (CS), an unique optimization algorithm known as Rider Integrated Cuckoo Search (RI-CS) is used in this study to discover the best route to choose with the lowest routing cost [274]. An improved hybrid ant colony optimization routing protocol (EHACORP) was created to improve the efficiency of the shortest path routing technique [275]. The shortest path of the proposed protocol has the smallest number of hops between source and destination vehicles and has the smallest communication cost. The EHACORP is composed of two phases. The EHACORP employs a distance computation algorithm to establish the separation between cars in phase 1. Phase 2 uses source-based ant colony optimization to tell the ants to build a shorter path with fewer hops to convey data. The effectiveness of the regimen as a whole is increased by the shortest method.

5.6.3. Performance Metrics

Throughput

The term "throughput" refers to the volume of packets generated by the sender node over a predetermined period of time, and it describes the amount of data established over a destination. The formula is,

$$\begin{aligned} \text{Throughput} \\ &= \text{received data packet} \times 8 \\ &\quad / \text{data packet transmission period} \end{aligned}$$

Packet Delivery Ratio

It is a procedure utilized in the optimal analysis of incoming and outgoing network data packets. It is determined by dividing the number of packets produced by the source by the amount of data received from the vehicle. The calculation utilized to generate the PDR is,

$$PDR = \frac{\text{ReceivedPackets}}{\text{GeneratedPackets}} * 100$$

Drop

It represents the amount of packets dropped as a result of malicious nodes (DoS attack).

$$Drop = \frac{Send\ packet - Received\ packet}{Send\ packet}$$

Delay

A packet from its source to its destination, encounters delays

$$delay = \frac{length}{bandwidth}$$

5.6.4. Performance Analysis

This section describes about the performance of proposed methods through parameters such as Energy consumption, Drop, Delay, Throughput, packet delivery ratio, fairness index

PHASE 1

Phase I detects the DDoS attack using a novel machine learning technique called SVM-HHO, that provides the information about the vehicle. This section describes the analysis and the performance of proposed technique and is detailed below.

Table 5.3: Performances of proposed Approach

<i>Node</i>	<i>Energy Consumption (mJoules)</i>	<i>Drop[%]</i>	<i>Delay(s)</i>	<i>Throughput (kilo bytes/sec)</i>	<i>Network Lifetime</i>	<i>Packet Delivery Ratio (PDR)</i>	<i>Fairness Index (FI)</i>
Proposed Method							
20	0.25	1.6531	97	1278	339.52	20	4.2477
40	0.32	9.9854	37	1920	664.32	33	2.4125
60	0.35	14.6785	50	1710	524.00	48	1.7961
80	0.43	50.5456	95	1345	370.81	59	1.5752
100	0.51	57.1534	68	1209	307.71	64	1.3947

The performance measures' main objective is to evaluate the model's effectiveness in identifying DDoS attacks and allocating bandwidth in the context of VANET settings. From the Table: 5.3, the proposed modified machine learning-based hybrid optimization technique is more effective as compared and analyzed with existing approaches. The proposed methodology achieves energy consumption, delay ratio, and drop ratio of 0.35 J, 50, 14.6785 in node 60th. Additionally, the suggested method provides Throughput of 1710 Mbps.

5.6.5 Energy Consumption

a) Overall energy consumption

The overall energy consumption of proposed method from the table 5.3, is plotted and detailed in graph below

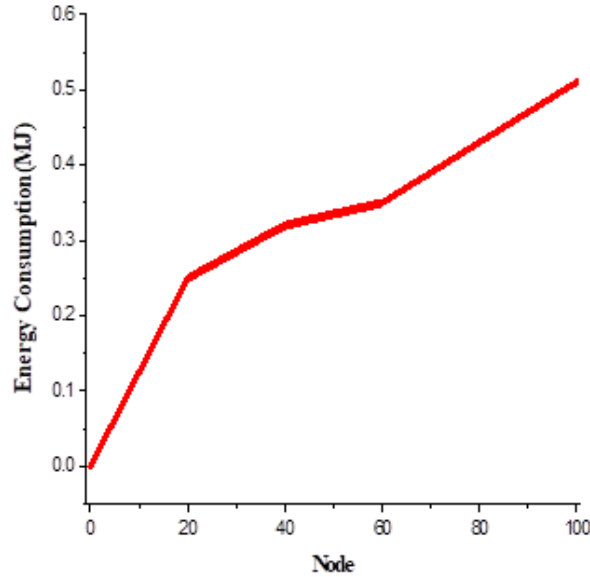


Figure 5.8: Energy consumption of proposed method

From the figure 5.8, the energy consumption of proposed method is plotted in graph. The rate of energy consumption on each node is noted. At node 100th, energy consumption of 0.5 is habited. The increase of node with increase in energy consumption.

b) Data rate based Energy Consumption

From table 5.4, the energy consumption of proposed method is tabulated at each node with data set. Node with data set values is marked in table.

Table 5.4:Energy Consumption based on data rate

Node	D-4	D-6	D-8	D-10	D-12	D-14
20	0.8	1.2	1.6	2.1	2.5	2.9
40	0.4	0.6	0.8	1.1	1.2	1.5
60	0.5	0.8	1.0	1.2	1.6	1.8
80	0.7	1.1	1.5	1.9	2.3	2.6
100	0.9	1.3	1.8	2.3	2.7	3.2

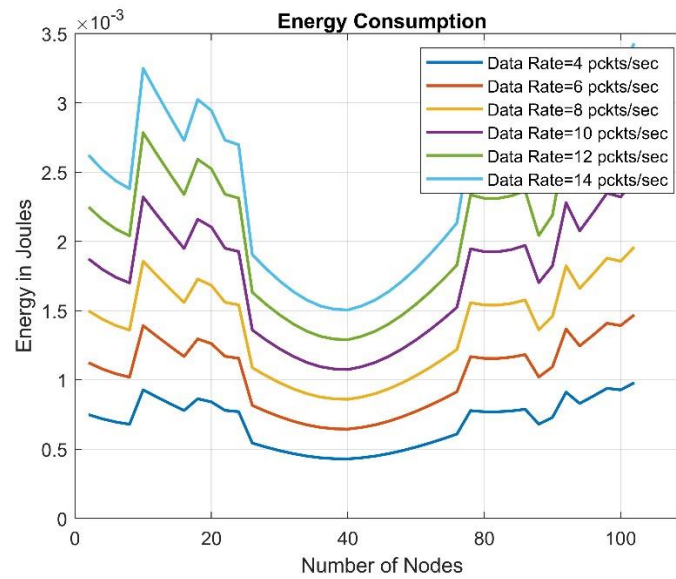


Figure5.9: Consumption of Energy based on data set

Figure:5.9 illustrates the energy consumption ratio of the proposed system, if the data packets rates are high the energy is in the peak, if not the energy produces lower data rates. From Table: 5.4, at node 20th, energy consumption is 0.8 is obtained in data rate-4, 1.2 is attained in data rate-6, 1.6 is acquired in data rate-8, 2.1 is accomplished in data rate-10. 2.5 is gained in data rate-12, 2.9 is fetched in data rate-14. Similarly, in node 40th, energy consumption is 0.4 in data rate-4, 0.6 in data rate-6, 0.8 in data rate-8, 1.1 in data rate-10,

1.2 in data rate-12, 1.5 in data rate-14. Moreover, at node 60th, energy consumption is 0.5 in data rate-4, 0.8 in data rate-6, 1.0 in data rate-8, 1.2 in data rate-10, 1.6 in data rate-12, 1.8 in data rate-14. In addition, at node 80th, energy consumption is 0.7 in data rate-4, 1.1 in data rate-6, 1.5 in data rate-8, 1.9 in data rate-10, 2.3 in data rate-12, 2.6 in data rate-14. Furthermore, at node 100th, energy consumption is 0.9 in data rate-4, 1.3 in data rate-6, 1.8 in data rate-8, 2.3 in data rate-10, 2.7 in data rate-12, 3.2 in data rate-14.

5.6.6 Network Lifetime

a) Overall Network lifetime

The overall network lifetime of proposed method from the table 5.3, is plotted and detailed in graph below

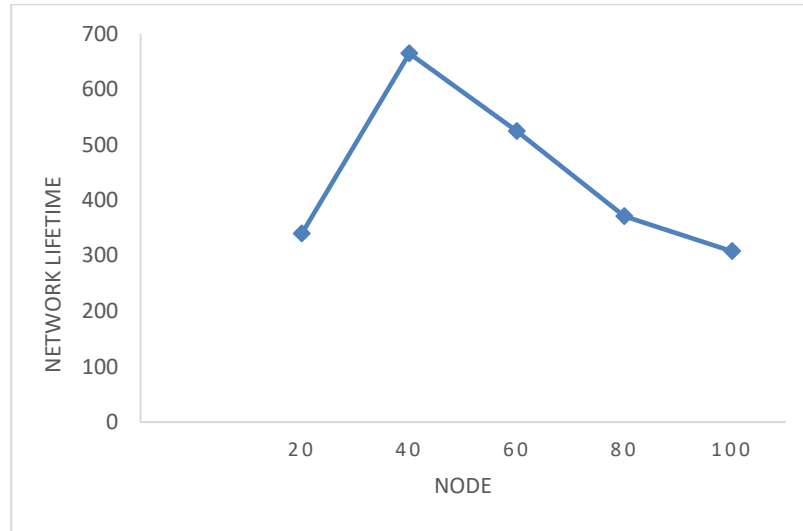


Figure 5.10: Network lifetime of proposed method

From the figure 5.10, the Network life time of proposed method is plotted in graph. The rate of Network life time on each node is noted. At node 100th, Network life time of 307.71 is habited. The increase of node with increase in network lifetime.

b) Data Rate based Network lifetime

From table5.5, the network lifetime of proposed method is tabulated at each node with data set. Node with data set values is marked in table.

Table 5.5: Lifetime of Network

<i>Node</i>	<i>D-4</i>	<i>D-6</i>	<i>D-8</i>	<i>D-10</i>	<i>D-12</i>	<i>D-14</i>
20	339.5	396.1	475.3	594.2	792.2	1188
40	664.3	775	930.1	1163	1550	2325
60	554.2	646.5	816.3	969.8	1293	1940
80	370.2	432.6	519.1	648.9	865.2	1298
100	307.7	359	430.8	538.5	718	1077

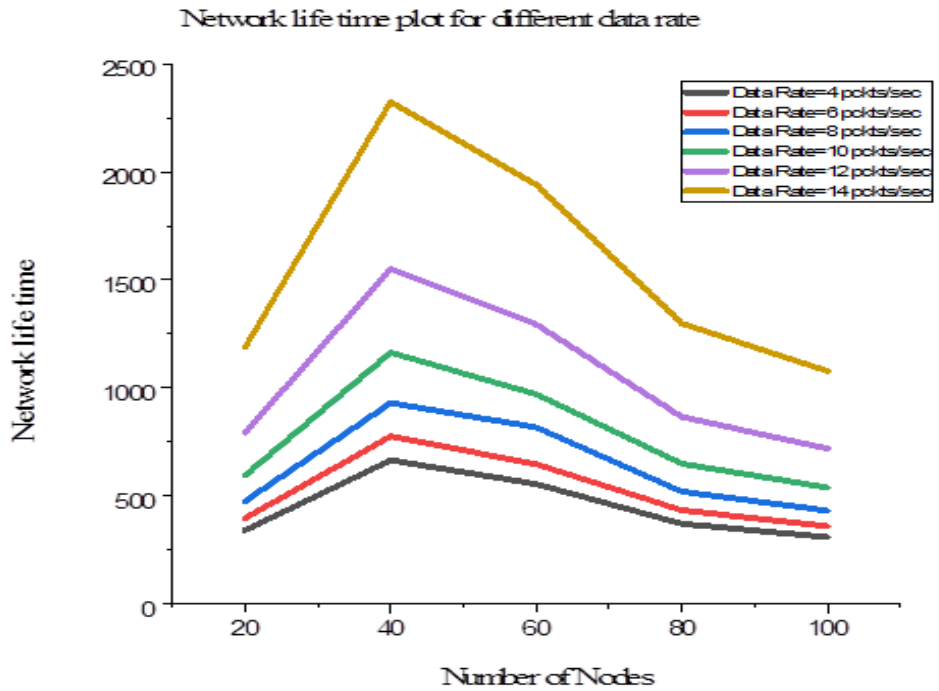


Figure5.11: Network Life-Time

Figure: 5.11 demonstrate the network lifetime of the proposed system, in which if the data packets rate is low, the network lifetime appears high. From Table: 5.5, at node 20th, network lifetime 339.5 is obtained in data rate-4, 396.1 is attained in data rate-6, 475.3 is acquired in data rate-8, 594.2 is accomplished in data rate-10. 792.2 is gained in data rate-12, 1188 is fetched in data rate-14. Similarly, in node 40th, network lifetime is 664.3 in data rate-4, 775 in data rate-6, 930.1 in data rate-8, 1163 in data rate-10, 1550 in data rate-12, 2325 in data rate-14. Moreover, at node 60th, network lifetime is 554.2 in data rate-4, 646.5 in data rate-6, 816.3 in data rate-8, 969.8 in data rate-10, 1293 in data rate-12, 1940 in data rate-14. In addition, at node 80th, network lifetime is 370.2 in data rate-4, 432.6 in data rate-6, 519.1 in data rate-8, 648.9 in data rate-10, 865.2 in data rate-12, 1298 in data rate-14. Furthermore, at node 100th, network lifetime is 307.7 in data rate-4, 359 in data rate-6, 430.8 in data rate-8, 538.5 in data rate-10, 718 in data rate-12, 1077 in data rate-14.

5.6.7. Throughput

a) Overall Throughput

The overall Throughput of proposed method from the table 5.3, is plotted and detailed in graph below.

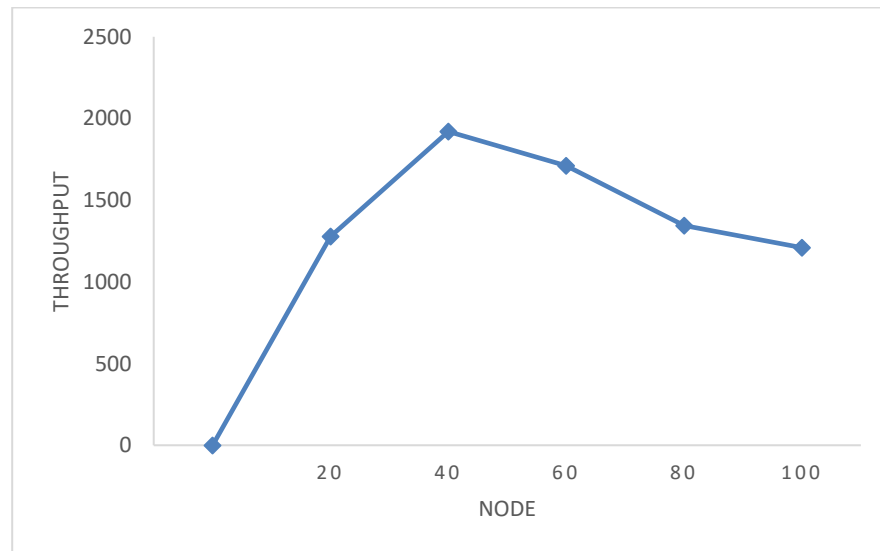


Figure 5.12: Through put of proposed method

The proposed method's throughput is represented in a graph in figure 5.12. The rate of Throughput on each node is noted. At node 100th throughput of 1209 is habited. The increase of node with increase in Throughput.

b)Data rate based Throughput

From table 5.6, the throughput of proposed method is tabulated at each node with data set. Node with data set values is marked in table.

Table 5.6:Throughput based data set

Node	D-4	D-6	D-8	D-10	D-12	D-14
20	12700	19180	25570	31960	38350	44740
40	19200	28800	38400	48000	57600	67280
60	17100	25650	34200	42750	51300	61700
80	13450	20170	26890	33620	40340	47060
100	12090	18140	24180	30230	36280	42320

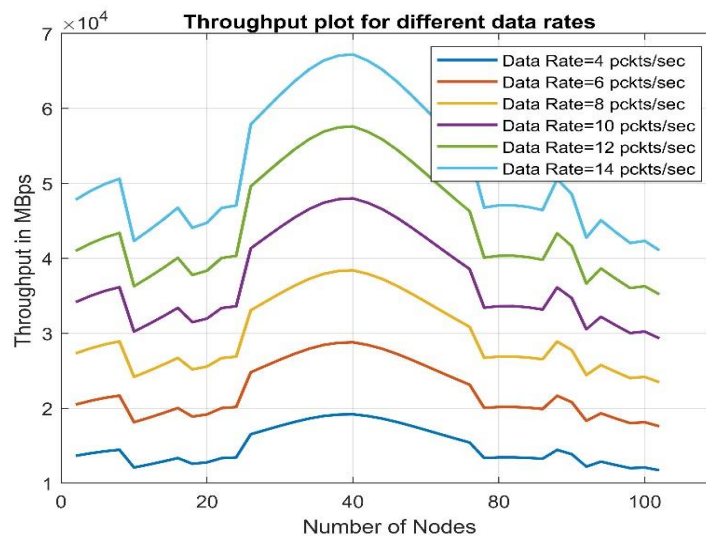


Figure 5.13: Plot for Throughput

Figure:5.13 demonstrates the throughput ratio of the proposed system. In which if the data packets rates were low then the throughput ratio also lower. The throughput of the proposed technique is reached by 42320 in node 100th at data rate of 14 packets/sec. At node 20th, 12700 throughput is obtained in data rate-4. At node 20th, 19180 throughput is attained in data rate-6. At node 20th, 25570 throughput is acquired in data rate-8. At node 20th, 31960 throughput is accomplished in data rate-10. At node 20th, 38350 throughput is gained in data rate-12. At node 20th, 44740 throughput is fetched in data rate-14. Similarly, in node 40th, 19200 throughputs in data rate-4, 28800 throughputs in data rate-6, 38400 throughputs in data rate-8, 48000 throughputs in data rate-10, 57600 throughputs in data rate-12, 67280 throughputs in data rate-14, and at node 60th, 17100 throughputs in data rate-4, 25650 throughputs in data rate-6, 34200 throughputs in data rate-8, 42750 throughputs in data rate-10, 51300 throughputs in data rate-12, 61700 throughputs in data rate-14. In addition, at node 80th, 13450 throughputs in data rate-4, 20170 throughputs in data rate-6, 26890 throughputs in data rate-8, 33620 throughputs in data rate-10, 40340 throughputs in data rate-12, 47060 throughputs in data rate-14. Furthermore, at node 100th, 12090 throughputs in data rate-4, 18140 throughputs in data rate-6, 24180 throughputs in data rate-8, 30230 throughputs in data rate-10, 36280 throughputs in data rate-12, 42320 throughputs in data rate-14.

5.6.8. Packet Delivery Ratio (PDR)

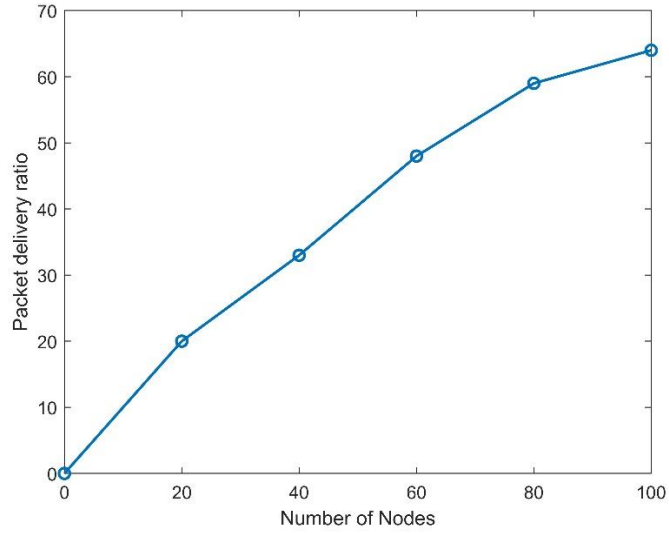


Figure 5.14: Ratio of Packet Delivery

Figure: 5.14 illustrates the packet delivery ratio. To an optimized analysis of incoming and outgoing network packets, the PDR is evaluated to assess the process. In VANET scenario, the packet deliver ratio represents the greater presentation of the system.

PHASE 2

Phase 2 contains the findings and analysis of the suggested and implemented strategies for strengthening machine learning with a hybrid optimization strategy to predict mobility in VANET. The execution of the work (H-WDFOA - VANET) is evaluated and compared to that of existing methods (RI-CS, EHACORP). Measurable metrics for latency, energy consumption, drop, throughput, and fairness index are generated in order to contrast the proposed (H-WDFOA-VANET) and existing (RI-CS, EHACORP) technologies. The implementation is done out using the NS2 stimulator and is based on a number of performance indicators, such as delay, energy consumption, drop, throughput, and fairness index. This analysis yielded a number of conclusions, which are summarized and described in the subsections that follow.

1) Results obtained through node

In terms of delay, energy utilization, drop, throughput, and fairness index, the node of the proposed methodology is compared to the nodes of the existing methodologies. The table below provides examples of the measured values. Table 5.7 displays the node values for both current and forward-looking methods.

Table 5.7: Comparison with existing approaches through nodes

Performance Parameters	Techniques	Nodes			
		20	40	60	80
Delay(s)	H-WDFOA-VANET[Proposed]	0.299063	10.05305	15.61668	15.64318
	RI-CS[274]	10.22709	29.63915	46.23192	46.03685
	EHA-CORP[275]	6.942181	17.167577	20.178139	19.568945
Energy consumption(MJoules)	H-WDFOA-VANET[Proposed]	7	3	2	2
	RI-CS[274]	8	5	4	3
	EHA-CORP[275]	8	4	3	2
Drop(%)	H-WDFOA-VANET[Proposed]	0.66674	0.17871	0.15759	0.15504
	RI-CS[274]	0.99904	0.6142	0.4456	0.3898
	EHA-CORP[275]	0.99293	0.521614	0.340694	0.308867
Throughput (Mbps)	H-WDFOA-VANET[Proposed]	41661	27995	30560	40095
	RI-CS[274]	13582	18785	20202	22299
	EHA-CORP[275]	25022	22043	26556	31937
Fairness Index (FI)	H-WDFOA-VANET	66	17	15	15
	RI-CS[274]	99	61	44	38
	EHA-CORP[275]	99	52	34	30

The proposed H-WDFOA is compared with the existing methods like RI-CS and EHA-CORP, through the parameter metrics like Delay, Energy consumption and Drop to prove that the presented model is better than other existing approaches. For Delay, in node 20th, the proposed is 0.299063 and the existing are 10.22709, 6.942181. In addition, at node 40th, value for delay in proposed is 10.05305 and the existing are 29.63915, 17.167577.

Also, at node 60th, for proposed value is 15.61668 and the existing are 46.23192, 20.178139. At node 80th, the proposed have 15.64318 and the existing have 46.03685, 19.568945 respectively. Delay is reduced while compared with the existing RI-CS and EHA-CORP with proposed H-WDFOA.

For Energy consumption values, at node 20th, the proposed is 7.00000 and the existing are 8.00000, 8.00000. In addition, at node 40th the proposed is 3.00000 and the existing are 5.00000, 4.00000. Also, at node 60th, value for proposed is 2.00000 and the existing are 4.00000, 3.00000. At node 80th, the proposed have 2.00000 and the existing have 3.00000, 2.00000 respectively. Energy consumption is reduced while compared with the existing RI-CS and EHA-CORP from proposed H-WDFOA.

For Drop, at node 20th, the proposed method value is 0.66674 and the existing are 0.99904, 0.992930. In addition, at node 40th, the proposed is 0.17871 and the existing are 0.6142, 0.521614. Also, at node 60th, for proposed is 0.15759 and the existing are 0.4456, 0.340694. At node 80th, the proposed have 0.15504 and the existing have 0.3898, 0.308867 respectively. Drop is reduced while compared with the existing RI-CS and EHA-CORP from proposed H-WDFOA.

The primary goal of the performance metrics is to assess how well the suggested model is able to predict VANET mobility. Table 5.7 demonstrates that the proposed method outperforms and is evaluated with existing methodologies when machine learning is enhanced with a hybrid optimization strategy to predict mobility in VANET.

The proposed H-WDFOA is compared with the existing methods like RI-CS and EHA-CORP, through the parameter metrics like Throughput and Fairness Index to prove that the presented model is better than other existing approaches. For Throughput values, at node 20th, the proposed is 41661 and the existing are 13582, 25022. In addition, at node 40th, for proposed is 27995 and the existing are 18785, 22043. Also, at node 60th, for proposed is 30560 and the existing are 202302, 26556. At node 80th, the proposed have 40095 and the existing have 22299, 31937 respectively. Throughput is increased while compared with the existing RI-CS and EHA-CORP from proposed H-WDFOA. For Fairness Index, at node

20th, the value for the proposed is 66 and the existing are 99, 99. In addition, at node 40th, for proposed is 17 and the existing are 61, 52. Also, at node 60th, for proposed value is 15 and the existing are 44, 34. At node 80th, the proposed have 15 and the existing have 38, 30 values respectively. Fairness Index is reduced while compared with the existing RI-CS and EHA-CORP from proposed H-WDFOA.

The nodes of the existing approaches and the proposed technique are compared in terms of delay, energy consumption, drop, throughput, and fairness index. The measured values are plotted in the ensuing images:

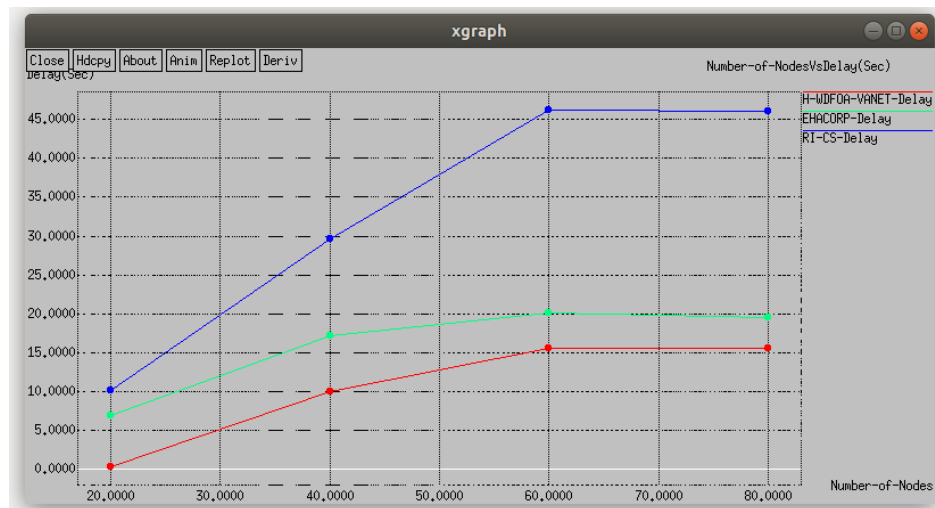


Fig 5.15: Node Vs Delay plot for proposed and existing method

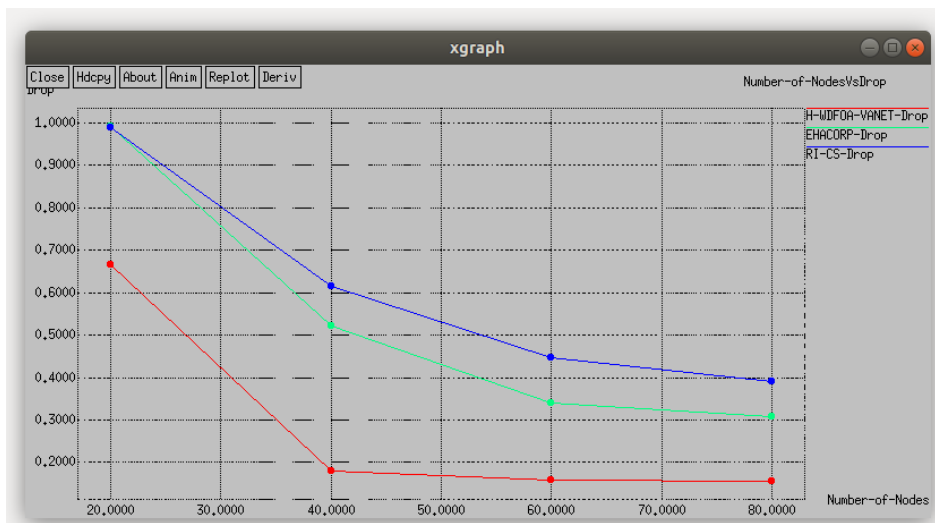


Fig 5.16: Node Vs Drop plot for a proposed and existing method

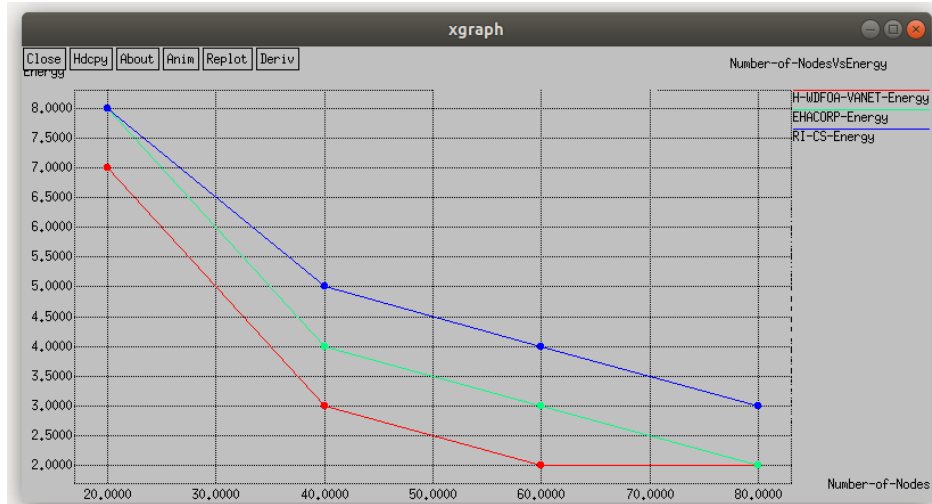


Fig 5.17: Node Vs energy consumption plot for a proposed and existing method

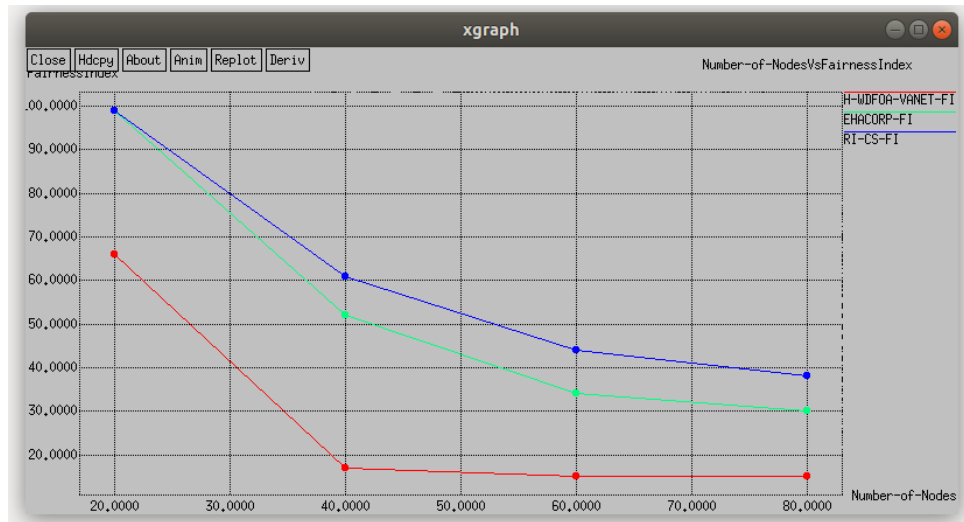


Fig 5.18: Node Vs Fairness Index plot for a proposed and existing method

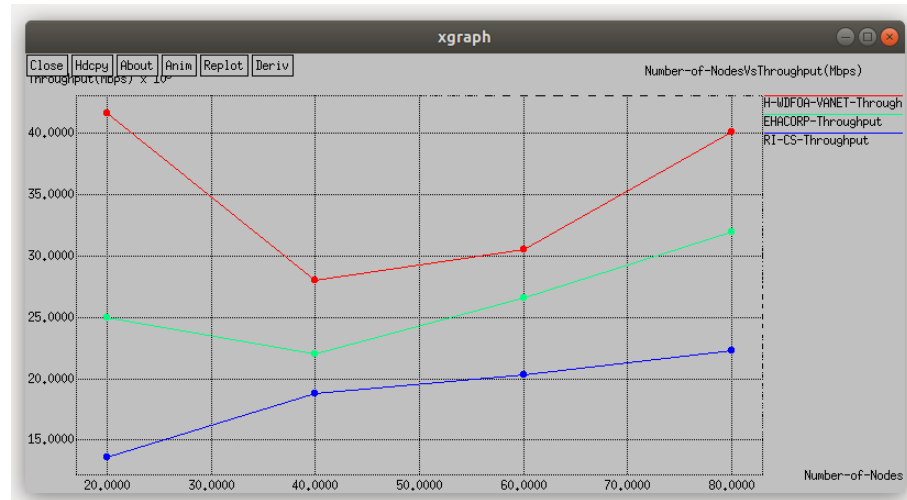


Fig 5.19: Node Vs Throughput plot for a proposed and existing method

2) Result obtained through speed

On the basis of delay, energy use, drop, throughput, and the fairness index, the suggested technique's speed is compared to the speeds of the existing techniques. The table below provides examples of the measured values. The speed values for both the current and the suggested approaches are shown in Table 5.8.

Table 5.8: Comparison of the proposed method to existing methods of speed

Performance Parameters	Techniques	Speed			
		20	40	60	80
Delay(s)	H-WDFOA – VANET[Proposed]	90.180295	395.189005	924.638246	1227.591591
	RI-CS[274]	138.843616	686.703072	1210.68834	1565.515813
	EHA-CORP[275]	100.98126	502.120993	1037.0019	1251.455006
Energy consumption(Joules)	H-WDFOA – VANET[Proposed]	1320	680	900	1200
	RI-CS[274]	1980	2440	2640	3040
	EHA-CORP[275]	1980	2080	2040	2400
Drop(%)	H-WDFOA – VANET[Proposed]	13.334678	7.151254	9.450511	12.405151
	RI-CS[274]	19.80027	24.58287	26.7894	31.195048
	EHA-CORP[275]	19.858595	20.86455	20.441628	24.709388
Throughput(Mbps)	H-WDFOA – VANET[Proposed]	199	24	14	10
	RI-CS[274]	16	5	2	1
	EHA-CORP[275]	96	21	10	6
Fairness Index (FI)	H-WDFOA – VANET[Proposed]	3	2	1	1
	RI-CS[274]	4.0746	2.819775	2.0302	1.672425
	EHA-CORP[275]	6	3	2	2

To demonstrate that the suggested H-WDFOA is superior to other existing ways, it is compared to existing techniques like RI-CS and EHA-CORP using parameter metrics like Delay, Energy usage, and Drop. For Delay, at speed 20th, the proposed value is 90.180295 and the existing are 138.843616, 100.981260. In addition, at speed 40th, for proposed value is 395.189005 and the existing are 686.703072, 502.120993. Also, at speed 60th, for proposed value is 924.638246 and the existing are 1210.688340, 1037.001897. At speed 80th, the proposed have 1227.591591 and the existing have 1565.515813, 1251.455006 respectively. Delay is reduced while compared with the existing RI-CS and EHA-CORP with proposed H-WDFOA.

For Energy consumption, at speed 20th, the proposed value is 1320 and the existing are 1980, 1980. In addition, at speed 40th, the proposed is 680 and the existing are 2440, 2080. Also, at speed 60th, for proposed is 900 and the existing are 2640, 2040. At speed 80th, the proposed have 1200 and the existing have 3040, 2400 respectively. Energy consumption is reduced while compared with the existing RI-CS and EHA-CORP from proposed H-WDFOA.

For Drop, at speed 20th, the proposed is 13.334678 and the existing are 19.80027, 19.858595. In addition, at speed 40th, the proposed is 7.151254 and the existing are 24.582870, 20.864550. Also, at speed 60th, for proposed is 9.450511 and the existing are 26.78940, 20.44162. At node 80th, the proposed have 12.405151 and the existing have 31.195048, 24.709388 respectively. Drop is reduced while compared with the existing RI-CS and EHA-CORP from proposed H-WDFOA.

The proposed H-WDFOA is compared with the existing methods such as RI-CS and EHA-CORP in terms of the parameter metrics such as Throughput and Fairness Index to prove that the presented model is better than other existing approaches. For Throughput, at speed 20th, the proposed value is 199 and the existing are 16, 96. In addition, at speed 40th, for proposed is 24 and the existing are 5, 21. Also, the speed at 60th, for proposed is 14 and the existing are 2, 10. At speed 80th, the proposed have 10 and the existing have 1, 6 values respectively. Throughput is increased while compared with the existing RI-CS and EHA-CORP from proposed H-WDFOA. For Fairness Index, at speed 20th, the proposed value is 3.00000 and the existing are 4.074600, 6.000000. In addition, the speed at 40th, for proposed value is 2.00000 and the existing are 2.8197750, 3.000000. Also, at speed 60th, for proposed is 1.00000 and the existing are 2.030200, 2.000000. At node 80th, the proposed have 1.00000 and the existing have 1.672425, 2.000000 respectively. Fairness Index is reduced while compared with the existing RI-CS and EHA-CORP from proposed H-WDFOA.

The speed is contrasted with the delay, energy, drop, throughput, and fairness index in the graph below.

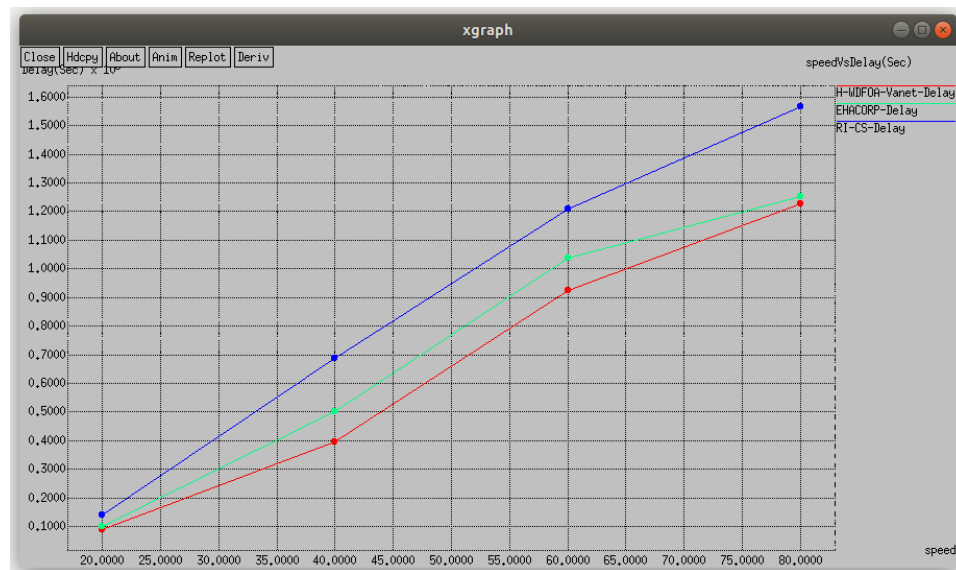


Fig5.20: Speed Vs Delay plot for proposed and existing method

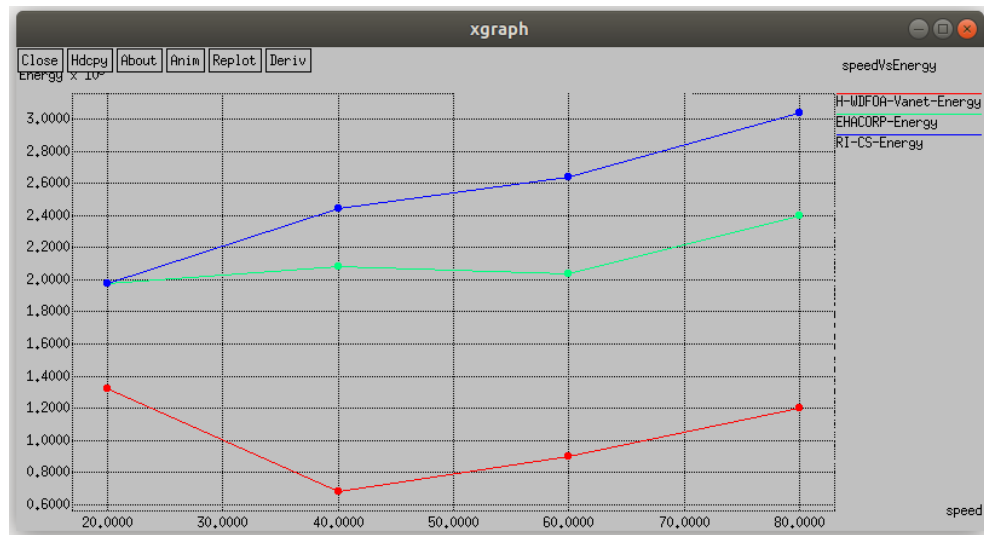


Fig 5.21: Speed Vs energy consumption plot for a proposed and existing method

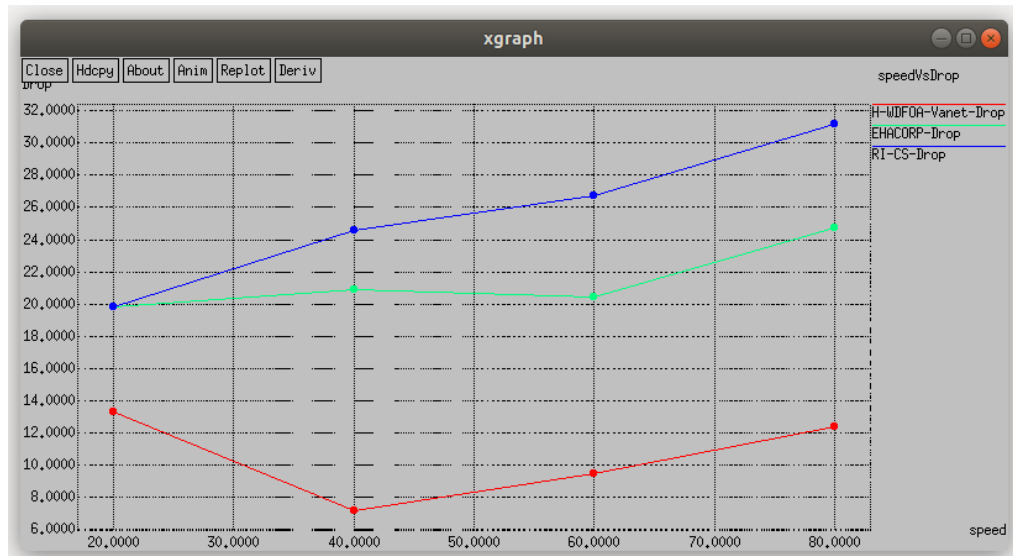


Fig 5.22: Speed Vs Drop plot for a proposed and existing method

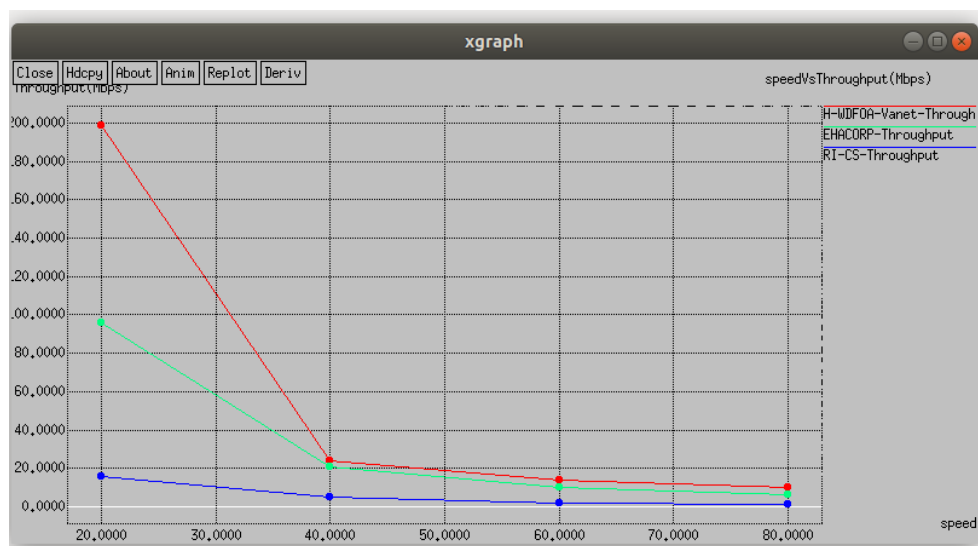


Fig 5.23: Speed Vs Throughput plot for a proposed and existing method

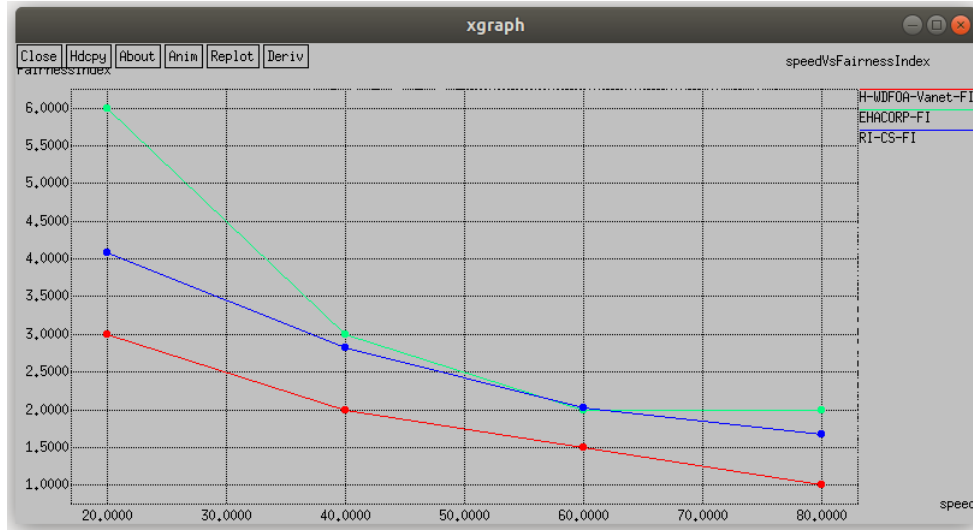


Fig 5.24: Speed Vs Fairness index plot for a proposed and existing method

5.7 Summary

This research project is primarily concerned with the allocation of bandwidth in the VANET and the detection of DDoS attacks using a machine learning-hybrid optimization technique. The detection of DDoS attack is performed through the SVM-HHO technique i.e., Modified SVM. Then the impact of DDoS attack in the VANET is mitigated through a Hybrid Whale Dragonfly Optimization technique (H-WDFOA-VANET). This work uses a novel optimization algorithm called Hybrid Whale Dragonfly Optimization technique (H-WDFOA-VANET), which hybridises the idea of Rider Integrated Cuckoo Search, to discover the best route with the lowest routing cost (RI-CS). After validation, a quick and trustworthy communication is established for stability in vehicle networks in order to use the predicted information. The proposed method's performance is estimated by evaluating the performance metrics such as, energy consumption, throughput, latency, and packet delivery ratio. This study suggests a brand-new routing protocol named H-WDFOA-VANET to boost the effectiveness of routing in VANETs. In the H-WDFOA-VANET, the DCM and SBACO combo speed up convergence, prevent blind broadcasting of packets, process packets more quickly, and prevent stagnation issues. The packet delivery ratio and

throughput in the H-WDFOA-VANET are improved by using the shortest channel without stagnation, swift packet processing, and quick convergence speed. Finally, the effectiveness of the proposed Hybrid Whale Dragonfly Optimization approach (H-WDFOA-VANET) is compared to other popular models like the Enhanced Hybrid Ant Colony Optimization Routing Protocol and Rider Integrated Cuckoo Search (RI-CS) (EHACORP). Throughput is achieved using the suggested method, which is better than the previous method. At node 60th, the suggested system obtains energy consumption values of 2.00000mJ, 15.61668s, and 0.15759. The new strategy also achieves a higher throughput than the previous one. The provided approach in node 60th successfully achieves energy usage, delay value, and drop value. The suggested approach achieves energy consumption, delay value, and drop value in the 80th node at 2.00000mJ, 15.64318s, and 0.15504, respectively. As a result, the proposed method shows an effective outcome. Therefore, when compared to existing systems, the suggested system's performance is found to be more efficient.

CHAPTER 6

ENSEMBLE APPROACH TO ANALYZE HYBRID METAHEURISTIC ENHANCED APPROACH TO ACHIEVE NETWORK STABILITY

6.1 Introduction

The last 10 years have seen intense study on connected and automated vehicles (CAVs), which aim to address a number of issues with intelligent transportation systems (ITSs). The development of ITS based on wireless communication networks is receiving substantial attention from numerous researchers, companies, and governments around the world [276, 277]. Wireless networks link vehicles to facilitate information exchange, enhancing driver and passenger convenience and security. In the VANET, broadcasting is a typical strategy. Three domains are used to categorize VANET components:

- There are one or more application units (AUs) and one on-board unit in the in-vehicle domain (OBU). A dedicated device known as an AU can either be a built-in component of a vehicle or a standalone portable device like a smartphone, laptop, etc. It utilizes the OBU communication capabilities by running one or more apps. Through a wired or wireless connection, the AUs and OBU are always linked.
- The ad-hoc domain is made up of moving Road-Side Units (RSUs) stationed along the roadside and equipped with OBUs. Using wireless short-range communication devices that enable ad hoc communications between vehicles, OBUs can communicate with one another either directly or over a multi-hop connection. An RSU is a stationary device that can be connected to the Internet or a network of infrastructure. It enables the ad-hoc network's reach to be expanded by sending, receiving, or forwarding data in the ad-hoc domain (i.e., in vehicles with OBUs and RSUs). To communicate with Internet nodes or servers, an OBU can connect to the Internet via an RSU

connected to the infrastructure, a public or private wireless Hot Spot (HS), or both. [278].

- HSs and RSUs are used to access the infrastructure domain. In the absence of Internet access through RSUs or HSs, OBUs can make use of cellular radio networks like HSDPA, WiMax, and 4G.

In addition to providing advertisements and notifications, broadcasting can be used to exchange transportation, weather, traffic, and crisis-related data amongst cars. because of a number of things, including an extremely dynamic topology, frequent disconnections, enough energy, and other things. There are significant variations between mobile ad hoc network routing and broadcast routing in VANET (MANET). Therefore, developing a powerful routing system for VANET is essential. Routing research faces a variety of difficulties as a result of the frequent dynamic changes in topology caused by the fast movement of VANET vehicles. For instance, in a VANET, vehicular traffic is often restricted to bidirectional movements on roads and highways [279–280]. The roads and streets in VANET, which have a tendency to be predictable, serve to restrict vehicle activity. Each vehicle can then keep track of both its present position and its past travels. By doing this, vehicles may predict how they and their neighbours will move in the future.

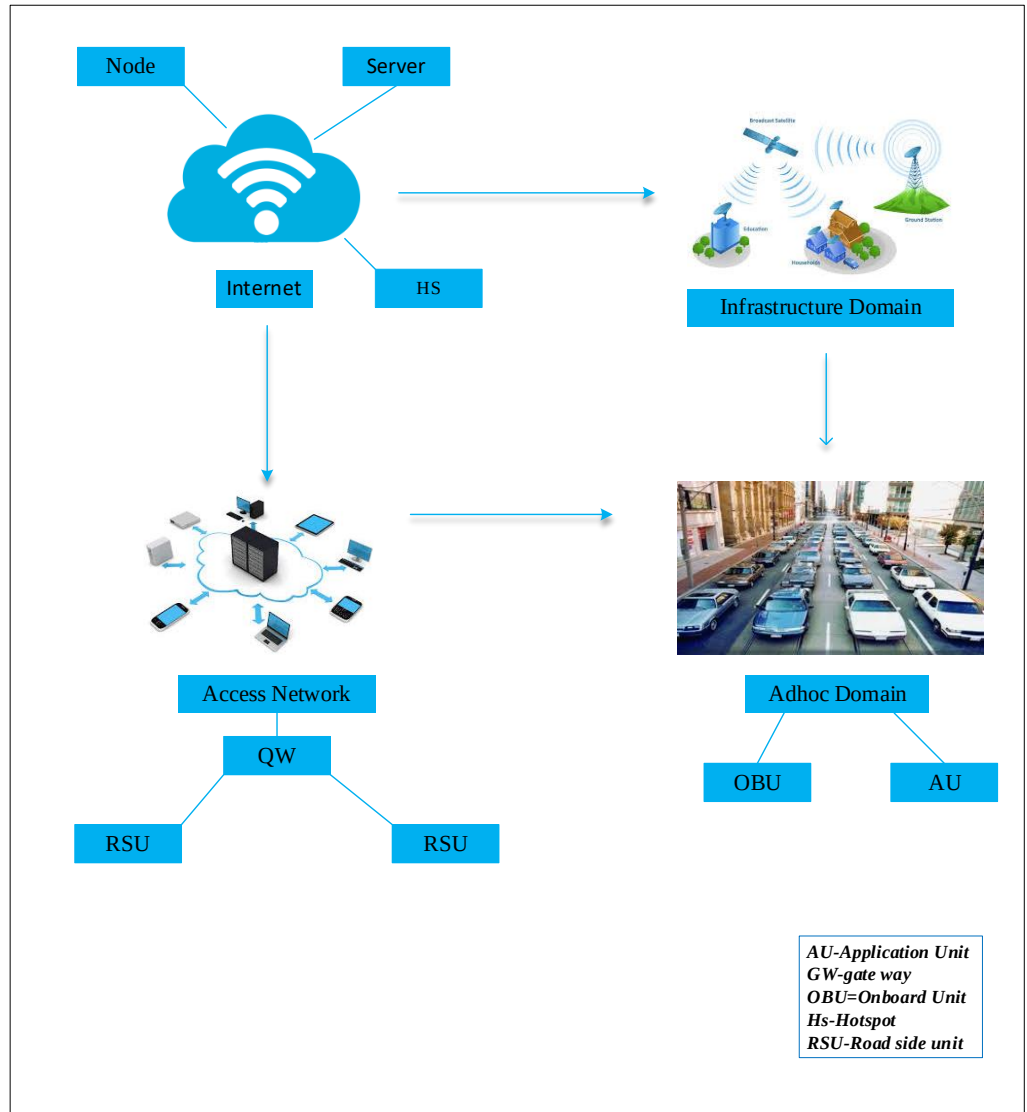


Figure 6.1: Architecture of VANET

Furthermore, it is assumed that the communications partner's positional coordinates are already known in position-based routing. Position-based routing is hence regarded as one of the most advantageous VANET technologies. There is a lot of research on broadcast strategies for ad hoc networks [281]. They focus their efforts on a small number of solutions that better fulfill the needs of VANETs because of the limited amount of space available. Flooding is an easy way to create a broadcast service, in which every car broadcasts messages to all of its neighbours in addition to the one it received from [282]. Flooding

achieves good performance even with a limited number of nodes by ensuring that the message eventually reaches every node in the network. Additionally, it is simple to use. Performance, however, drastically degrades as the network's nodes multiply. Position-based schemes require nodes to be aware of that position in order to have a higher tolerance for node movement [283]. As a result, the farthest node is always picked first, and rebroadcast nodes are employed to increase the area covered by each transmission. For example, the Urban Multi-Hop Broadcast (UMB) protocol is intended for broadcast propagation in automotive networks [284-285]. Every hop in UMB involves at least two-way handshakes as the source nodes attempt to rebroadcast the message to the farthest node in the broadcast direction. The UMB protocol outperforms the 802.11-distance and 802.11-random protocols in conditions of high packet loads and vehicle traffic densities [286-289]. Depending on the congestion resolution algorithm, the potential relay nodes wait the longest before retransmission. In situations when there is a high level of mobility, this approach can result in a large delay. Position-based broadcast techniques like History-enhanced (HV-TRADE) and Vector-based Tracking Detection (V-TRADE) are also recommended. Their main assessment is comparable to the GPS-based unicast routing method [290].

Highlights of this chapter are as follows:

- ❖ A machine-learning system based on ensemble learning which was developed to forecast VANET mobility.
- ❖ Based on information from the Road Side Unit (RSU) or the Base Station, the estimation is carried out using a hybrid metaheuristic method, such as Seagull optimization and Artificial fish swarm optimization (BS).
- ❖ Migration and Attacking are two factors that contribute to the cluster leader's proper evaluation. The Migration phase begins with gulls migrating from a location to another.
- ❖ The artificial fish swarm algorithm (AFSA) is a novel design technique that produces a school of artificial fish that closely replicates the traits of actual fish in freshwater. Through low-level, straightforward behaviour and individual

connections, the method reveals the group's high artificial intelligence execution on a macro level.

6.2. Literature Review

This section mostly discusses research publications based on VANET in the literature. A QoS-aware and secure routing algorithm was developed in 2021 by Nadarajan, J. et al [291] using the next-generation VANET. Adaptive Routing based on Stochastic Chaos with Prediction (SCARP). With the aid of potent deep learning networks, SCARP promotes a stochastic-based node discovery routing approach in order to produce accurate traffic flow predictions. The technique reduced connectivity loss, lowered latency, and granted chaotic authentication to construct an effective and secure data transmission system among car nodes.

The hybrid machine learning-based model that was used to duplicate and assess the task of a rare car traffic flow forecast system was first introduced by Boukerche, A. et al. in 2020 [292]. To put the model into practice, the emphasis is on enhancing the traits of the prediction model. The present a novel hybrid deep learning model based on the deep aggregation structure of the Gated Recurrent Unit (GRU) and the Graph Convolutional Network (GCN). For the online prediction challenge, the online prediction technique is based on refinement learning. To improve the model's precision and effectiveness while utilizing the structure of the vehicular cloud, an effective parallel training technique is used with ITS.

The cognitive radio vehicular network was introduced in 2021 by Hossain, M.A., et al [293] using machine learning-based cooperative spectrum sensing in dynamic segmentation. Roads are divided into equal pieces and then partitioned based on the probability value. Certain vehicles or other users deliver local sensing data using a hybrid machine learning technique that combines fuzzy and naive Bayes algorithms to determine the optimum spectrum sensing (SS) approach. To make the overall decision in cooperative SS, the

segment spectrum agent (SSA) employed the tri-agent reinforcement learning (TA-RL) technique.

A future intelligent and secure automobile network in the 6G era was presented with machine-learning algorithms in 2019 by Tang, F., et al [294]. It becomes hard to achieve the severe requirements of the next-generation (6G) network, such as ultralow latency, high reliability, high safety, and gigantic connections, as the automobile network gets diversified, active, and mass-scale. A potent artificial intelligence (AI) technology known as machine learning (ML) has arisen as a means of improving the capability and flexibility of wireless communication as well as automobiles. Intelligent radio (IR) network development, self-learning with proactive exploration and various machine learning techniques applied to communication, networking, and security components in vehicular networks are being pursued in order to enable artificial intelligence (AI) in a future 6G vehicular network.

The best technique to enhance blockage control in 5G IoT (Internet of Things) networks' wireless sensors was evaluated in 2019 by Najm, I.A., et al [295]. Using a training dataset, the model was utilized to determine the ideal parametric configuration for a 5G scenario. The data was used to create a machine learning model that predicted the best options and enhanced the effectiveness of the obstruction control strategy. Any user can use the graphs provided by DT (decision tree) algorithms to comprehend how the prediction method functions.

The study of Wireless Ad Hoc Networks, a Futuristic Analysis of Machine Learning-Based Routing Protocols, by Kaushik, S., et al. [296] was conducted in 2021. Investigations are conducted on how machine learning impacts various wireless ad-hoc networks and how performance parameters change as a result. All simulators that are employed and evaluated by various protocols in MANET and VANET are investigated methodically. After choosing the best machine learning model, users must ensure optimization by looking into a number of other factors and using simulations in ad-hoc networks to reduce the likelihood of data failure and boost throughput.

Ye, M., Guan, L. et al. presented a routing protocol using Mpbrp-mobility prediction in 2019. Using driver intent obtained from positioning devices, an unique Mobility Prediction Based Routing Protocol (MPBRP) was created for vicinity recognition, packet transmission, and path recovery in VANETs. A recovery mechanism and a predictive forwarding approach are coupled to find neighbours and send packets. Consider the driver's objective at a specified time by using the expected location and angles to select the nearby nodes and locate the transmission line. The suggested routing protocol outperforms existing ones in terms of packet delivery percentage and end-to-end latency, increasing overall execution.

The VANETs, an efficient clustering technique for connected and autonomous autos that was based on mobility prediction, were presented in 2019 by Abdel-Halim, I.T., et al [298]. A revolutionary system was MPECS (Mobility Prediction-based Efficient Clustering Scheme). The MPECS intended to divide the entire region into several portions using a Voronoi diagram, allowing each vehicle to anticipate its lifetime and cost of serving as the cluster leader. Additionally, MPECS was compared to four current VANET clustering algorithms, and the performance of MPECS was assessed using simulation. The test results show that simulation and analytical findings are very consistent, proving that MPECS may significantly boost clustering architectural stability with little overhead.

Rehman, O., et al. [299] researched the VANETs in 2020 and looked into how mobility speed affected communication in general. The performance of the farthest distance and connection quality-based strategies, two extensively used VANET messaging systems, was examined for the impact of vehicle speed differences. The explored approaches are created using a sender-oriented relay selection mechanism to make the best use of channel bandwidth. When it comes to message reachability, the connection quality method outperforms the longer distance approach in both speed difference scenarios. As a result, compared to the longer distance plan, the link quality was more resistant to the adverse effects of extreme differences in mobility speed.

2019 saw the use of the robust VANET performance estimation by Abdellah, A.R., et al [300]. A common back propagation learning approach employed by neural networks is

minimized using the training data mean square error (MSE). The VANET performance in terms of packet loss ratio and output was improved by using robust neural network learning based on the robust M-estimators presentation function rather than the standard MSE performance function. Robust M-estimators performance functions are surpassed by MSE performance functions in terms of RMSE and training duration.

6.3. Proposed Methodology

6.3.1 Background model of the Seagull Optimization algorithm

The Seagull Optimization Algorithm (SOA), which aids in the appropriate selection of the cluster leader, contains two crucial processes: migration and attacking. The Migration phase first mimics gulls flying from one location to another. The Seagull's three primary objectives are to avoid collisions, fly toward ideal neighbours, and remain close to the most effective search agent. Laridae, the formal name for seagulls, is a family of seabirds that inhabits the entire world. There are numerous species of seagulls, each with a unique bulk and length. As omnivores, seagulls consume a variety of foods, including worms, fish, amphibians, reptiles, and insects. Most seagulls have white feathers covering their bodies. Birds like seagulls are highly intelligent.

They utilize bread crumbs to entice fish, and they use the sound of their feet making rain to entice earthworms that are buried beneath the surface. Both fresh and salt water are consumable by seagulls. The majority of animals are incapable of doing this. Seagulls, on the other hand, have a particular pair of glands located directly over their eyes that are intended to flush the salt from their bodies through apertures in the bill. Seagulls typically reside in colonies. They hunt for their prey and attack it using their intellect. The main characteristics of seagulls are their migration patterns and aggressive tendencies. Migration is the term used to describe the seagulls' seasonal movement from one location to another in search of the richest and most plentiful food sources that will give them enough energy. This conduct is described as follows:

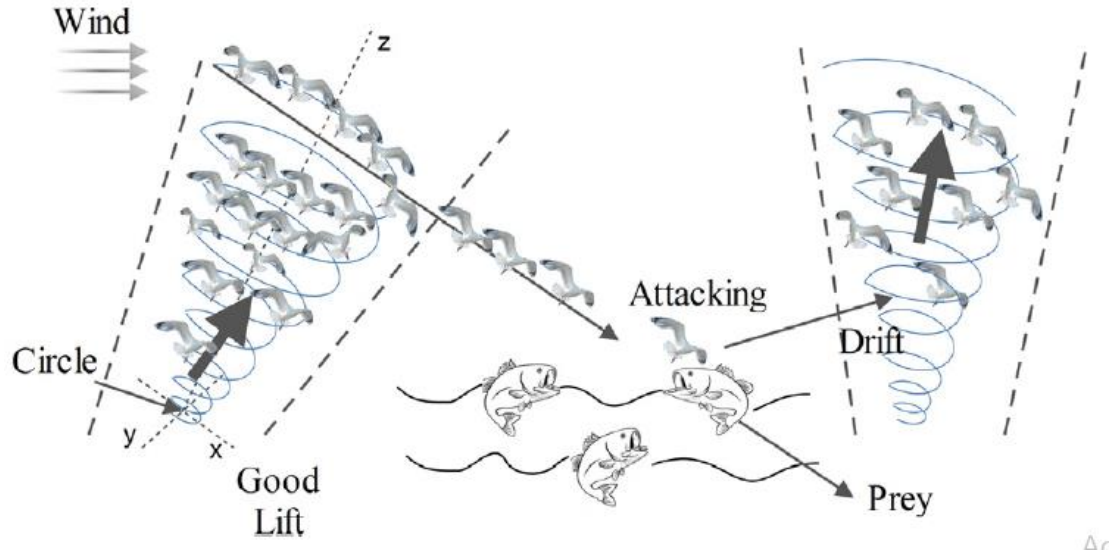


Figure 6.2: *Seagull Optimization algorithm*

- ❖ They migrate together as a group. In order to prevent collisions, seagulls start off in different locations.
- ❖ In a group, seagulls can move in the direction of the seagull with the best chance of surviving, or one whose fitness value 1 is lower than the others.
- ❖ Seagulls can adjust their starting positions based on the fittest one..

When birds move from one point to another over the sea, seagulls frequently attack the birds. They have the ability to manoeuvre in a spiral pattern naturally when attacking. Fig. 6.2 presents a conceptual picture of these behaviours. These behaviours may be expressed in a fashion that allows them to be connected to the objective function that has to be optimized. This enables the creation of a fresh optimization algorithm. This piece focuses on two seagull natural behaviours.

A) Collision Avoidance

The collision between neighbour search agents is reduced in this stage using additional variable A^* . The position of the new search agent, denoted by the " A^* ," is determined by,

$$P_s^* = A^* \times P_s^*(x) \quad (6.1)$$

Although,

P_S^* displays a search agent's optimal position to avoid clashing with other search agents, $P_S^*(x)$ shows the search agent's location during the current iteration or position, and A^* shows the movement of search agents within a specific search space.

$$A^* = f_A - \left(X' \times \left(\frac{f_A}{MAX_{iter}^*} \right) \right) \quad (6.2)$$

To control the frequency of the variable “ A^* ”, “ f_A ” is used where f_A is set to be 2 then it will be reduced linearly to "zero". The search agent indicates in the best vicinity when the collision is prevented.

B) Movement towards best neighbors' direction

$$P_{SA} = B^* \times (P_{bs}^*(x) - P_S^*(x)) \quad (6.3)$$

Although,

P_{SA} presents the site of Search agent P_S^* to the best search agent position P_{bs}^* . The variable “ B^* ” is used at random to manage the balance between exploration and exploitation in this case. The following equation shows the mathematical derivation of B^* .

$$B^* = 2 \times A^{2*} \times RD \quad (6.4)$$

Although,

The RD symbol represents the random value [0,1]. The position of the search agent is finally updated using the following equation based on the best search agent.

C) Approaching the best position

$$D_S^* = |P_S^* + P_{SA}| \quad (6.5)$$

Although,

The distance between the search agent and the top search agent is shown by the symbol D_S^* .

This approach was developed after reviewing earlier search techniques. In the air, prey is attacked using the spiralling technique. The X', Y', and Z' planes are crucial in this technique. Each plane is described in the paragraphs that follow.

$$X' = R' \times \cos K' \quad (6.6)$$

$$Y' = R' \times \sin K' \quad (6.7)$$

$$Z' = R' \times K' \quad (6.8)$$

$$R' = U' \times e^{K'V'} \quad (6.9)$$

Where,

R' signifies that the related component is taken into account for each turn radius.

U' and V' , the spiral is formed by multiple turns in the search space. These consonants define the spiral form.

K' means a random number that range is $[0 \leq K' \leq 2\pi]$.

e is the base of the actual logarithm.

The equations (6.8) and (6.9) are utilized for updating the position of the search agent.

$$P_S^*(x) = (D_S^* \times X' \times Y' \times Z') + P_{bs}^*(x) \quad (6.10)$$

Where,

The best result, represented by P_S^* , is saved and updated for the other search agents.

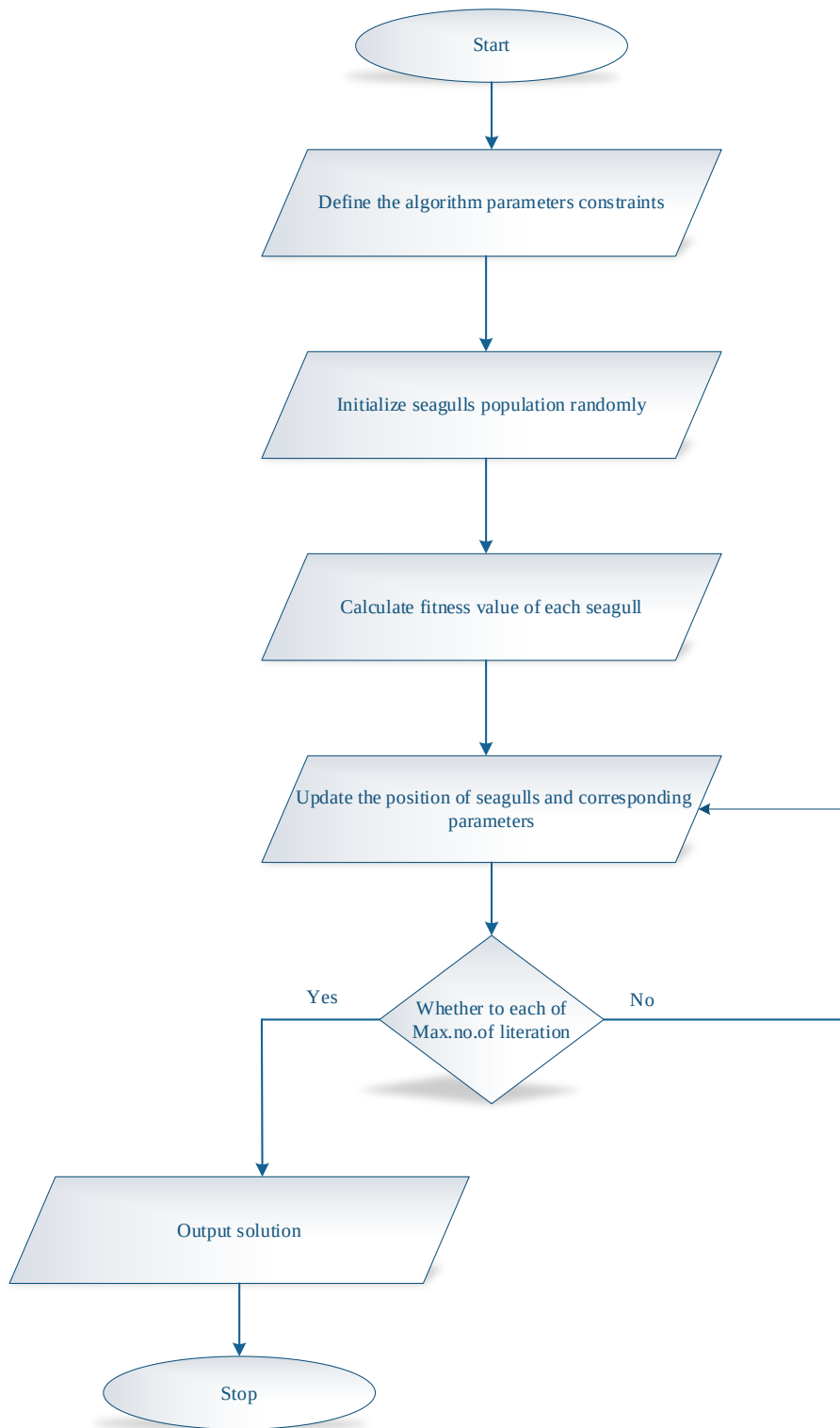


Figure 6.3: Flowchart of Seagull Optimization algorithm

6. 3.2 Improved artificial fish swarm algorithm

A unique design approach called the artificial fish swarm algorithm (AFSA) produces a swarm of artificial fish that matches the characteristics of actual fish in water. The programme reveals the group's high artificial intelligence behaviour on a macro level through straightforward low-level behaviour and local connections between individuals. It is described as local optimization of users and optimal global approximation of swarms in the algorithm optimization process. A set of randomly generated initial inhabitants are typically used in the standard AFSA methodology, which then converges to find the best resolution.

6. 3.2.1. Initialization

Consider the fish population, a starting representation of N nodes or vehicles, and the fact that the challenge at hand is a D-dimensional one. The fish swarm's state vector, which is best defined as, calculates the status of each individual fish:

$$X_i = (x_1, x_2, \dots, x_D) \quad (6.11)$$

The nodes or the state of the vehicle in this case indicate the state vector of the fish swarm. Then $Y_i = f(X_i)$ describes the meal pleasure (Qos (bandwidth, distance)) (X_i). The interaction between any two fish is described by the Euclidean distance, which is.

$$D_s^* = \|X_i - X_j\| \quad (6.12)$$

For $i, j = 1, 2, \dots, N$, X_i and X_j are the various states of the fish or nodes (Vehicles). The parameters that affect the algorithm's performance are the fish's visual field, the step size, and the degree of crowding, as expressed by the visual, step, and crowded factor, respectively. A description of AFSA's behaviour is depicted. The exploration activity of artificial fish toward a great meal is analogous to the approach activity of sensor nodes in sensor networks toward higher levels of network coverage. To choose the best feeding source, all artificial fish simply use the traits of randomness, predation, swarming, and following.

A) Vehicle position based on Improved Unspecified Conduct

Fish moving randomly in their area of vision is an example of random behaviour. The fish will select a state at random from its visual field if its current state i is P_s^* (Current State acquired from Seagull optimization). The movement procedure is as follows.

$$P_{s_next}^* = P_s^* + visual + Rand() \quad (6.13)$$

Here, the fish's visual field is indicated by Visual, and a random number between 0 and 1 is indicated by Rand(). With AFSO-VANET, the current vehicle location P_s^* , as determined by Seagull Optimization, will be improved.

B) Preying conduct

Fish moving haphazardly in the water, searching for food, and migrating in the direction of a location with a high food satisfaction is referred to as preying activity. If X_i represents the vehicle's current condition and X_j represents a randomly chosen new state inside its visual field, then:

$$X_j = P_s^* + visual * Rand() \quad (6.14)$$

Consider the case where $f(P_s^*)$ and $f(X_j)$ indicate, respectively, the states of P_s^* and X_j food enjoyment.

Case 1: X_j At its maximum, a fish takes one step in the direction of the next step, and its present state P_s^* next can be described as

$$X_{i_next} = P_s^* + \frac{P_s^* - X_j}{\|X_j - P_s^*\|} * step * Rand() \quad (6.15)$$

Case 2: $f(P_s^*) \geq f(X_j)$ The artificial fish reselects other states randomly. If the fish cannot meet the needs in a particular time, it moves one step randomly as (6.15)

Where $\|\cdot\|$ represents the artificial fish i and artificial fish j 's Euclidean distance.

Case 3: $f(P_s^*) \geq f(X_j)$ The artificial fish randomly chooses new states. The fish moves randomly one step if it cannot satisfy the needs at a specific time (6.15)

C) Collision avoidance in packed tendency to traffic management

There are many automobiles present in the VANET environment, which increases traffic and increases the risk of an accident. SOA technique increases the HFSA-intelligence VANET's in order to manage traffic utilizing the AFSA concept. Swarming tendency in an AFSA-based VANET refers to an artificial fish's propensity to group up and cluster near the nodes of its neighbours (vehicles). Let X_i represent the fake fish's current state, " P_s^* ", the updated optimal position of SEO, n_f the number of neighbour nodes in the visual area, and X_c the fellows' centre position state. The condition of the central position was calculated using the formula below:

$$X_c = \left(\sum_{j=1}^{n_f} \frac{X_j}{n_f} \right), D_{IJ} < visual \quad (6.16)$$

Euclidean distance between the artificial fish i and the artificial fish j is denoted by D_{ij} .

The uncrowded food satisfaction of center position state X_c is $f(X_c)$. If $f(X_c)/n_f > \delta f(P_s^*)$. Whereas δ is the crowded factor. If $f(X_c) \geq f(P_s^*)$ the fish moves one step ahead by the follows center position as follows:

$$P_{s^*/next}^* = P_s^* + \frac{X_c - P_s^*}{\|X_c - P_s^*\|} * step * Rand() \quad (6.17)$$

If this action is unsuccessful, the fish will engage in predatory behaviour. The degree of crowdedness effectively limits the size of swarms. The fish swarming scale increases with increased meal satisfaction. (The improved QoS value)

The Artificial Fish Swarm Optimization can be combined with the Seagull Optimization to effectively regulate the movements and collision avoidance of the vehicles.

D) Following Conduct

Their subsequent behaviour causes the artificial fish in their visual field with the highest food fulfilment to move closer to their area.

P_s^* , indicates the fake fish's current condition, and nf indicates how many objects are in its immediate vicinity in the visual field. At this instance, X_j represents the best fish (in the best food position) in X_i 's vision area. The food gratification of situation state X_j is $f(X_j)$. If $f(X_j) / nf > \delta f(P_s^*)$ and $f(X_j) > f(P_s^*)$, the fish moves one step forward X_j .

$$P_{s_next}^* = P_s^* + \frac{B^*(P_s^* - X_j)}{B^* \llbracket X_j - P_s^* \rrbracket} * step * Rand() \quad (6.18)$$

In order to enhance its performance based on the behaviour of the seagull optimization process, the variable B^* is added with the following behaviour in equation (6.18). When all of the algorithm's iterations have been completed, the algorithm is considered to have reached its optimal state, which is the state depicted on the noticeboard. In this case, the Cluster Head choice based on Fitness value is quite important. After that, the procedure is repeated for the neighbouring node to make sure that every node is given the highest fitness score. On the other side, a collective learning strategy is used to lessen the impact of a blackhole attack in network locations. An ensemble learning strategy based on ANN, SVM, DT, and RT algorithms is used to assess performance because this type of assault reduces the effectiveness of the network. The HFSA-VANET outcomes obtained in this model are assessed using all ensemble learning strategies. By recognizing and categorizing the attacks, each will produce a different set of findings, which will aid in deciding the optimum outcomes. The suggested model's flowchart demonstrates how the ensemble technique helped the model get better outcomes with HFSA-VANET. Figures 6.4 and 6.5, respectively, show the overall architecture and flowchart.

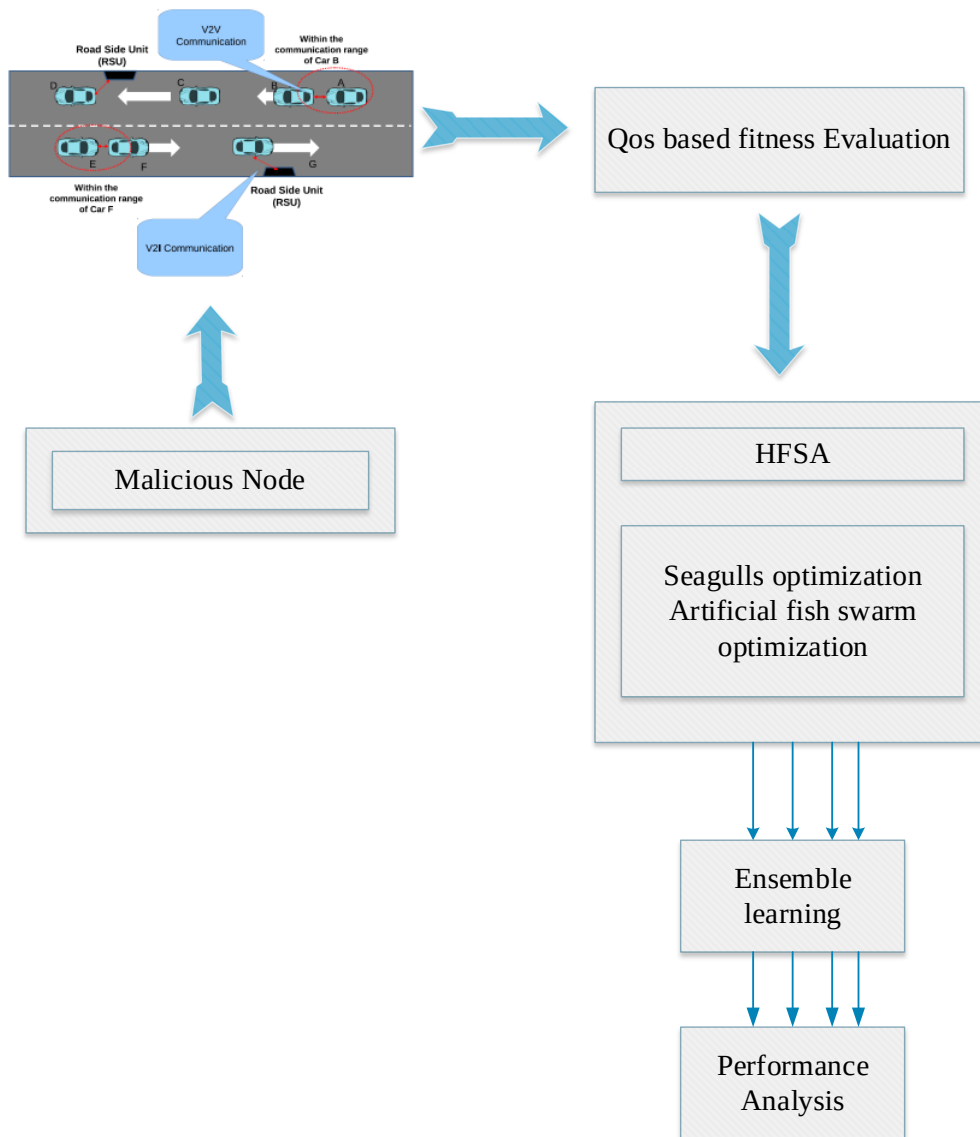


Figure 6.4: Overall architecture of the proposed model

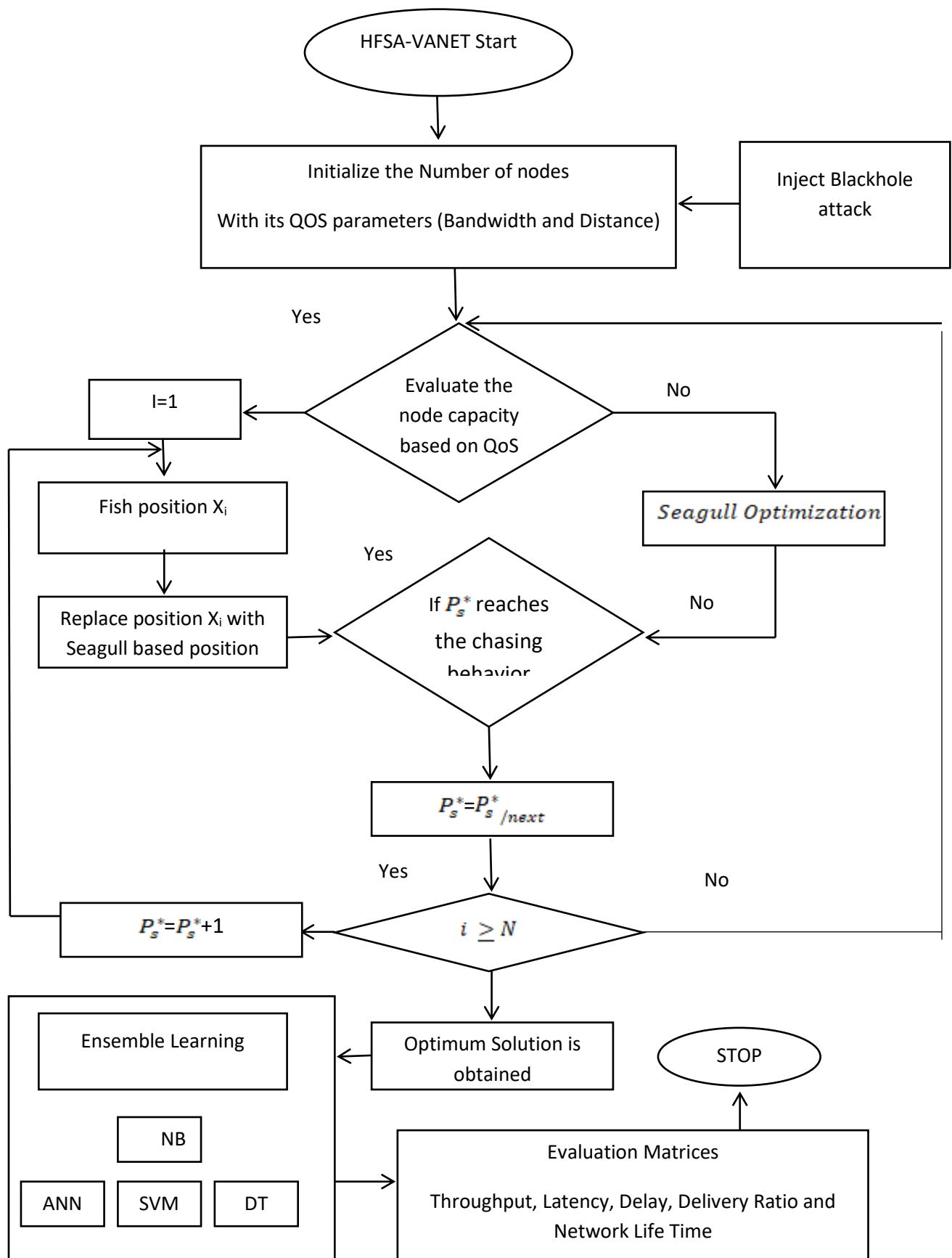


Fig 6.5:Flowchart for HFSA-VANET

6.3.3 Hybrid Seagull optimization and Artificial Fish Swarm Optimization

According to researchers, the artificial fish swarm optimization technique has significant drawbacks, including the ease with which local optimal values can be locked in and a lack of diversity. We proposed a hybrid seagull optimization with an artificial fish swarm strategy to make up for the deficiency, which dramatically improved foraging and random behaviour. The seagull is positioned in the position of the fish for this reason. The replacement role is listed as,

$$P_{bs}^*_{next} = P_{bs}^* + \frac{X_c - P_{bs}^*}{\|X_c - P_{bs}^*\|} * step * Rand() \quad (6.19)$$

The pseudo code procedure of the HFSA-VANET method is as follows:

Input: Initialization of population for the problem, visual, try number, crowd factor.

Initialization of X_i for each artificial fish AF_i ($i=1, 2, \dots, n$)

Output: Best Solution

Evaluate each AF_i , $F(X_i)$ ($i=1, 2, \dots, n$)

bulletin = min $F(X_i)$

while ($t < \text{Max Generation}$)

for each AF_i do

perform follow behavior on $X_i(t)$ and

compute ($X_{i, follow}$)

perform swarm behavior on $X_i(t)$ and

compute ($X_{i, swarm}$)

if $F(X_{i, follow}) < F(X_{i, swarm})$

```

 $X_i(t+1) = X_{i, follow}$ 

else

update the position by the seagull using (6.19)

end if

end for

if  $F(X_{best\_AF}) < F(bulletin)$ 

bulletin =  $X_{best\_AF}$ 

end if

end while

```

6.3.4 Existing Method

6.3.4.1. Centralized Routing Scheme with Mobility Prediction System (CRSM-VANET)

The CRSM routing method, in which the controller does not constantly track the whereabouts of the vehicles. The controller makes use of the ANN's strong learning capabilities to learn about and forecast the rate at which vehicles arrive. By developing a statistical traffic model based on the vehicle arrival rate function, the RSU/BS may estimate the mobility of the traffic and then decide how to route the cars. In contrast to V2I mode and V2V mode, the goal of the CRSM is to reduce the overall vehicular service latency. In V2I mode, the controller assists all cars in communicating through the RSU, but in V2V mode, all vehicles communicate by multi-hop transmission without the aid of the RSU. Traditional routing techniques typically perform worse as speed increases. However, our centralized routing system's performance is more reliable because it does not suffer significantly when the vehicle's speed rises, as shown in Figure 6.6.

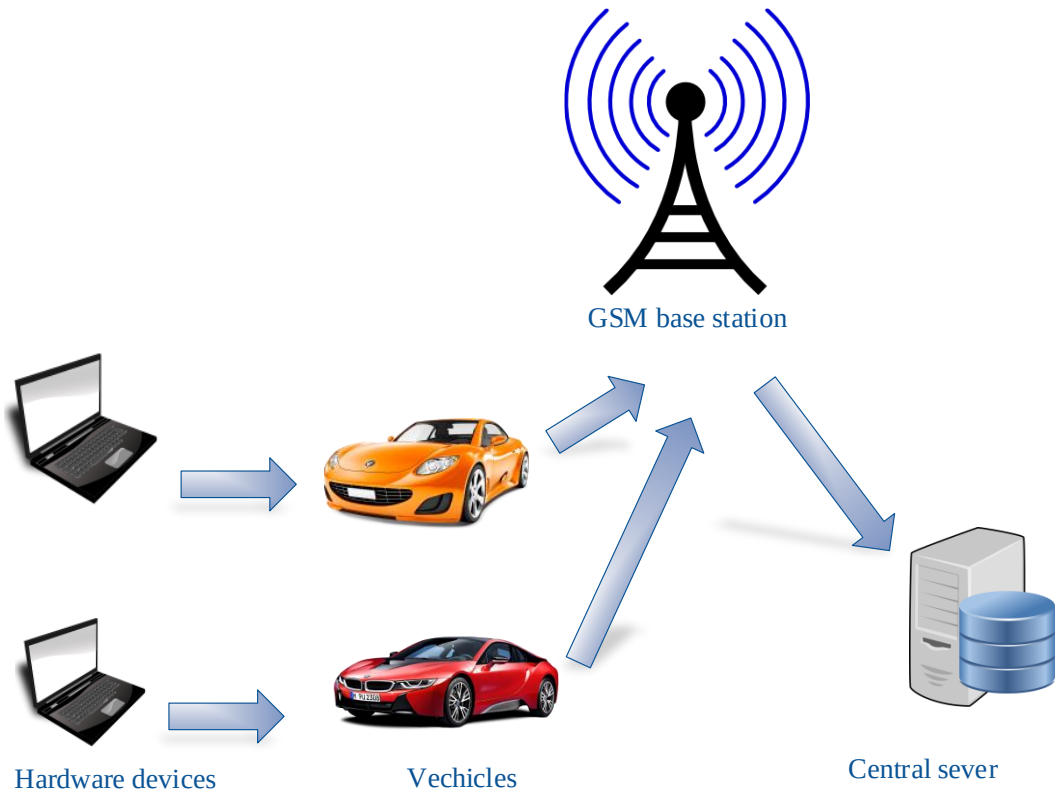


Figure 6.6: *Structure of CRSM*

In order to detect road vibration and determine position and vehicle velocity, CRSM modules are made up of an accelerometer and a GPS module. A lightweight data mining approach called i-GMM (improved Gaussian Mixture Model) is presented to detect road surface events and broadcast pothole information to the server in order to reduce storage and transmission expenses. To estimate the degree of road roughness, CRSM also offers a road roughness classification method. According to test results, CRSM can identify potholes in the road with an accuracy of up to 90% and almost no false alarms. Road roughness levels may be accurately assessed by CRSM as well, despite some influence from minor bumps or potholes.

6.3.4.2 Artificial Neural Network (ANN)

A computational model known as an artificial neural network (ANN) comprises of many processing components that accept inputs and produce results in accordance with predetermined activation functions. An artificial neural network, often known as a "neural network," is made up of three layers of neurons: an input layer of neurons (or nodes, units), one to three hidden layers of neurons, and a layer of output neurons at the top. A typical architecture is depicted in Figure 6.7, along with the connections between the neurons. Each connection has a weight that is a numeric value. The hidden layer's neuron i 's output, h_i , is,

$$h_i = \sigma\left(\sum_{j=1}^N V_{ij} x_j + T^{hid}_i\right) \quad (6.20)$$

Where N is the number of input neurons, V_{ij} are weights, x_j are inputs to the input neurons, and T^{hid}_i are the threshold terms of the hidden neurons, σ is known as the activation (or transfer) function. In addition to adding nonlinearity to the neural network, the activation function aims to constrain the neuron's value to prevent the neural network from being paralyzed by divergent neurons. The sigmoid (or logistic) function, which is a typical illustration of the activation function, is defined as (Figure 6.7).

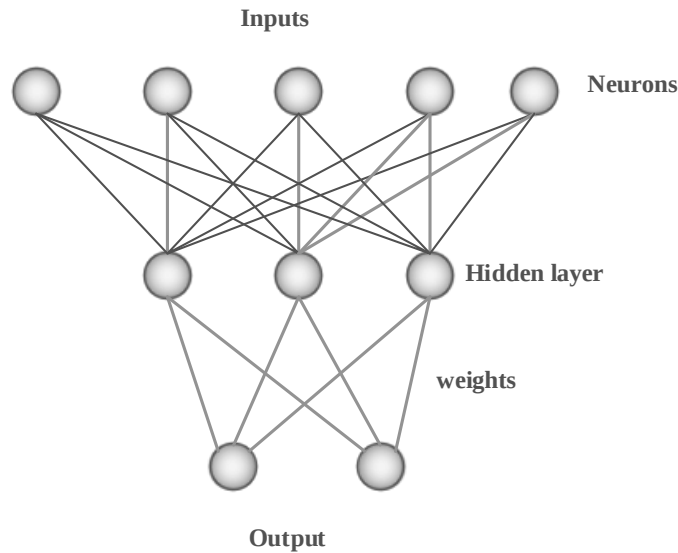


Figure 6.7:Architecture of Neural network

$$\sigma(\mu) = \frac{1}{1+\exp(-\mu)} \quad (6.21)$$

The arc tangent and hyperbolic tangent are additional potential activation functions. They respond to inputs similarly to the sigmoid function but have different output ranges. A neural network built in the manner described above has been demonstrated to be capable of approximating any computed function with arbitrary precision. For the function that the neural network is attempting to approximate, the numbers supplied to the input neurons are independent variables, and the numbers returned from the output neurons are dependent variables. When data is properly encoded, inputs to and outputs from a neural network can be binary (such as yes or no) or even symbols (green, red, etc.). This property gives neural networks a broad range of applications.

6.3.4.3 Support Vector Machine (SVM)

One of the traditional machine learning methods that can still be used to help with big data categorization issues is support vector machine. It can be especially useful for multi-domain applications in a huge data setting. The support vector machine is, nevertheless, computationally and theoretically demanding. The SVM algorithm's objective is to establish the best line or decision boundary that can divide n-dimensional space into classes, allowing us to quickly classify fresh data points in the future. A hyperplane is the name given to this optimal decision boundary.

SVM selects the extreme vectors and points that aid in the creation of the hyperplane. Support vectors, which are used to represent these extreme instances, form the basis for the SVM method. Take a look at the diagram below, where a decision boundary or hyperplane is used to categorise two distinct categories:

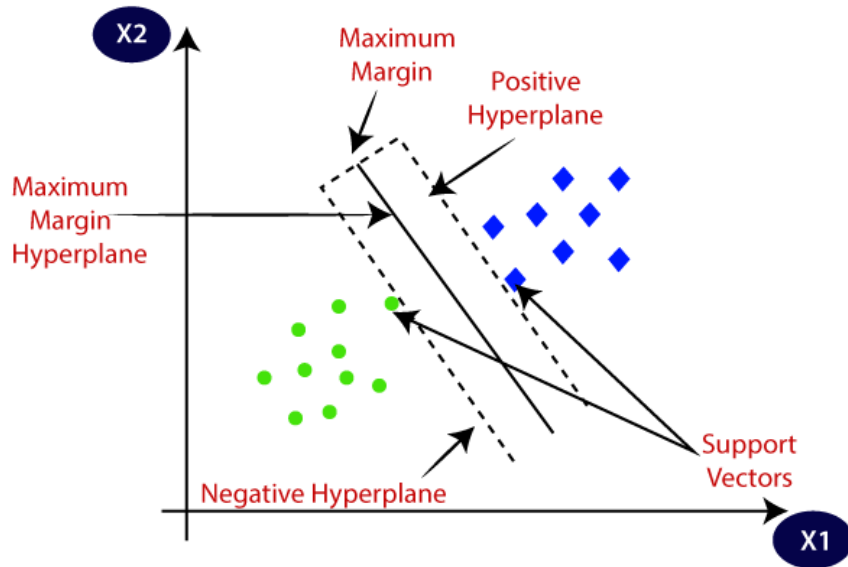


Figure 6.8: Mechanism structure of SVM

6.3.4.4 Naive Bayes (NB)

A similar approach is used by Naive Bayes to forecast the probability of various classes based on various attributes. The main application of this approach is text classification, which has issues with having several classes.

$$P(c|x) = \frac{P(x|c)P(c)}{P(x)} \quad (6.21)$$

- ❖ $P(c|x)$ is the post-hoc likelihood of class (c, target) given predictor. (x, attributes).
- ❖ $P(c)$ is the class's earlier probability.
- ❖ $P(x|c)$ is the likelihood of a predictor given a class, which is the likelihood.
- ❖ $P(x)$ is the predictor's prior probability.

A given example that is described by its feature vector is given the most likely class using a Bayesian classifier. By assuming that characteristics are independent of class, learning such classifiers can be significantly sped up, that is

$$P(X|C) = \prod_{i=1}^n P(X_i/C) \quad (6.22)$$

Where, $X = (X_1, \dots, X_n)$ is a feature vector and C is a class. In spite of this irrational presumption, the resulting classifier, Naive Bayes, is very effective in practise, frequently outperforming much more sophisticated methods. Numerous real-world applications, such as text classification, medical diagnosis, and system performance monitoring, have shown that Naive Bayes is effective.

The following can be used to illustrate why Naive Bayes works well when feature dependencies are present: The effectiveness of the fit to a probability distribution is not always correlated with optimality in terms of zero-one loss (classification error) (i.e., the appropriateness of the independence assumption). As long as the most probable class is agreed upon by both the actual and estimated distributions, an optimal classifier is instead obtained. For some issue classes with a high degree of feature dependencies, such as disjunctive and conjunctive ideas, demonstrate Naive Bayes optimality.

6.3.4.5 Decision Tree (DT)

To decide whether to divide a node into two or more sub-nodes, decision trees employ a variety of techniques. The homogeneity of newly formed sub-nodes is increased by sub-node creation. In other words, we can claim that the node's purity improves in relation to the desired variable. The Decision Node and Leaf Node are the two nodes of a decision tree. While Leaf nodes are the results of decisions and do not have any more branches, Decision nodes are used to create decisions and have numerous branches.

- ❖ Based on the characteristics of the provided dataset, judgments or tests are run.
- ❖ Based on predetermined conditions, it provides a graphic representation of all potential solutions to a problem or choice.
- ❖ It is known as a decision tree because, like a tree, it begins with the root node and then grows to form more branches.
- ❖ The CART algorithm, which stands for Classification and Regression Tree algorithm, is used to construct a tree.
- ❖ A decision tree only poses a question and divides the tree into subtrees based on the response (Yes/No).

- ❖ The decision tree's general structure is depicted in the diagram below:

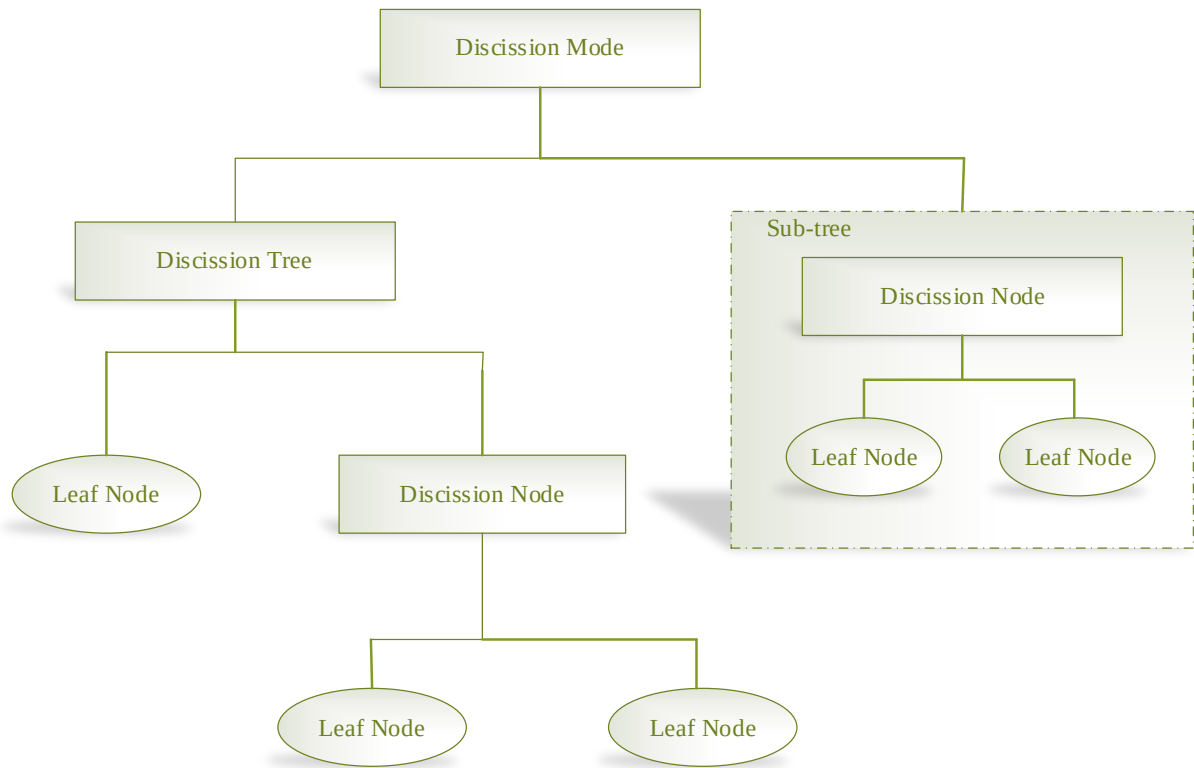


Figure 6.9: Structure of DT

The most important thing to keep in mind while developing a machine learning model is to select the optimal method for the dataset and task at hand. The two rationales for employing the decision tree are as follows:

- ❖ The theory behind the decision tree can be clearly understood because it displays a tree-like structure.
- ❖ Decision Trees typically replicate human thinking abilities while making a decision.

In a decision tree, the algorithm begins at the root node and works its way up to forecast the class of the given dataset. This algorithm follows the branch and jumps to the following node by comparing the values of the root attribute with those of the record (real dataset)

attribute. The algorithm verifies the attribute value with the other sub-nodes once again for the following node before continuing. It keeps doing this until it reaches the tree's leaf node. The following algorithm can help you better understand the entire procedure:

- **Step-1:** S advises starting the tree from the root node, which has the entire dataset.
- **Step-2:** Utilize Attribute Selection Measure to identify the dataset's top attribute (ASM).
- **Step-3:** Subsets of the S that include potential values for the best qualities should be created.
- **Step-4:** Create the best attribute-containing decision tree node.
- **Step-5:** Using the subsets of the dataset generated in step 3, repeatedly design new decision trees. Continue along this path until you reach a point when you can no longer categorise the nodes and you refer to the last node as a leaf node.

6.4 Section 1

The findings and analysis of the strategies for enhancing machine learning using a hybrid optimization strategy to forecast mobility in VANET are presented in Section 1. The work's execution (HFSA-VANET) is assessed and contrasted with the existing approach (CRSM-VANET). To compare proposed (HFSA-VANET) and current (CRSM-VANET) approaches, computations of the measured values of delay, energy consumption, drop, throughput, and fairness index are made. Additionally, the proposed technique is implemented using NS2 stimulation and compared with these two platforms using a Windows 10 PRO computer with a total RAM capacity of 10GB and an Intel TM core (7M) i3-6100CPU @ 3.70 GHz processor. The following section looks at performance metrics.

6.4.1. Performance metrics

Delay

A packet experiences delays as it moves from its source to its destination.

$$delay = \frac{length}{bandwidth} \quad (6.20)$$

Drop

It measures how many packets a rogue node has caused to be lost (DoS attack).

$$Drop = \frac{Send\ packet - Received\ packet}{Send\ packet} \quad (6.21)$$

Throughput

The throughput is the quantity of packet data established across a destination, which is equivalent to the total quantity of packets produced by the sender node over the course of a specific period of time. The equation reads as follows:

$$Throughput = received\ data\ packet \times 8 / data\ packet\ transmission\ period \quad (6.22)$$

The table below compares the performance metrics of the suggested method with those of the current technique.

Table 6.1: Comparison with existing approach

Node	Delay(s)		Energy consumption(Joules)		Drop(%)		Throughput(Mbps)		Fairness Index (FI)	
	HFSA-VANET {Proposed}	CRSM-VANET [164]	HFSA-VANET [Proposed]	CRSM-VANET [164]	HFSA-VANET [Proposed]	CRSM-VANET [164]	HFSA-VANET [Proposed]	CRSM-VANET [164]	HFSA-VANET [Proposed]	CRSM-VANET [164]
20	0.09369	2.123612	99	99	0.897708	0.998142	31341	30689	7	8
40	9.752925	12.431245	47	58	0.472094	0.586371	30573	29382	3	4
60	10.902826	13.786562	36	50	0.376633	0.514273	28423	26749	2	4
80	15.287826	20.464329	11	31	0.116375	0.310394	18197	16739	1	2

The main objective of the performance measures is to evaluate the proposed model's propensity to forecast VANET mobility. Table 6.1 shows that the suggested method, which enhances machine learning with a hybrid optimization strategy to predict mobility in VANET, performs better when compared to and tested with existing methodologies.

Below are comparisons between the CRSM-VANET and the HFSA-VANET in terms of throughput, throughput drop, energy consumption, latency, and fairness index.

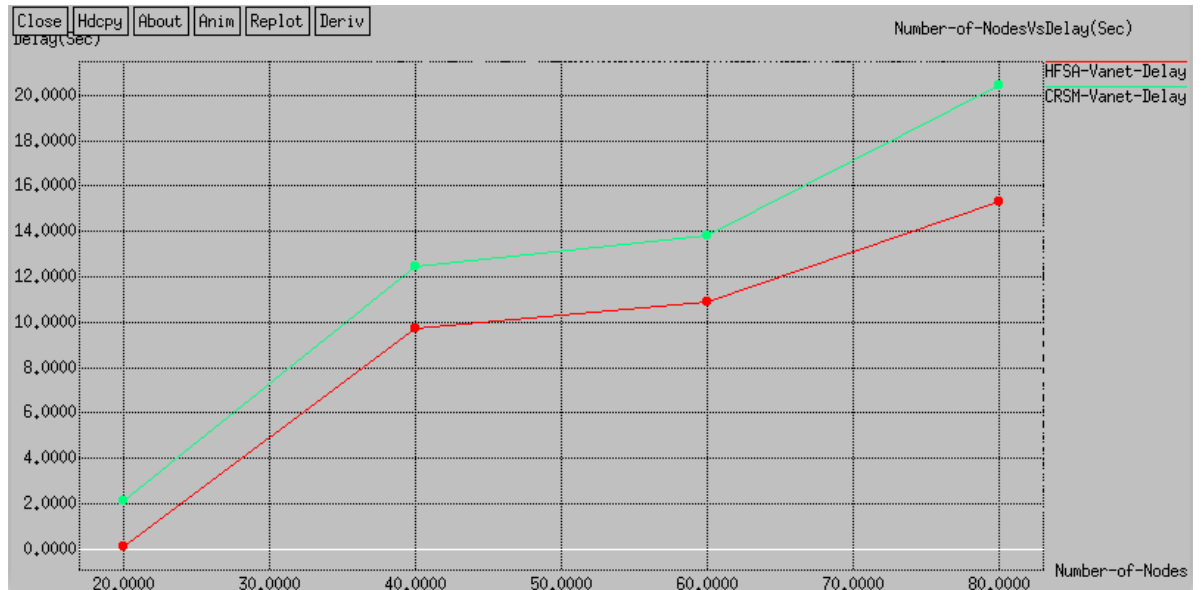


Figure6.10: Delay plot for a proposed and existing method

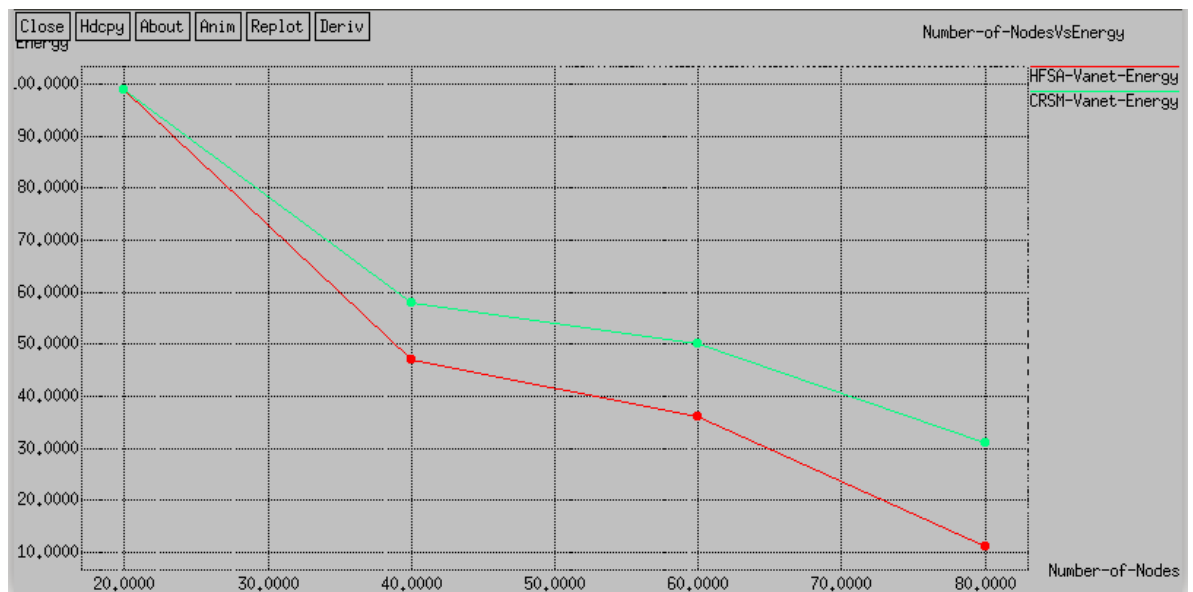


Figure6.11: Energy consumption plot for a proposed and existing method

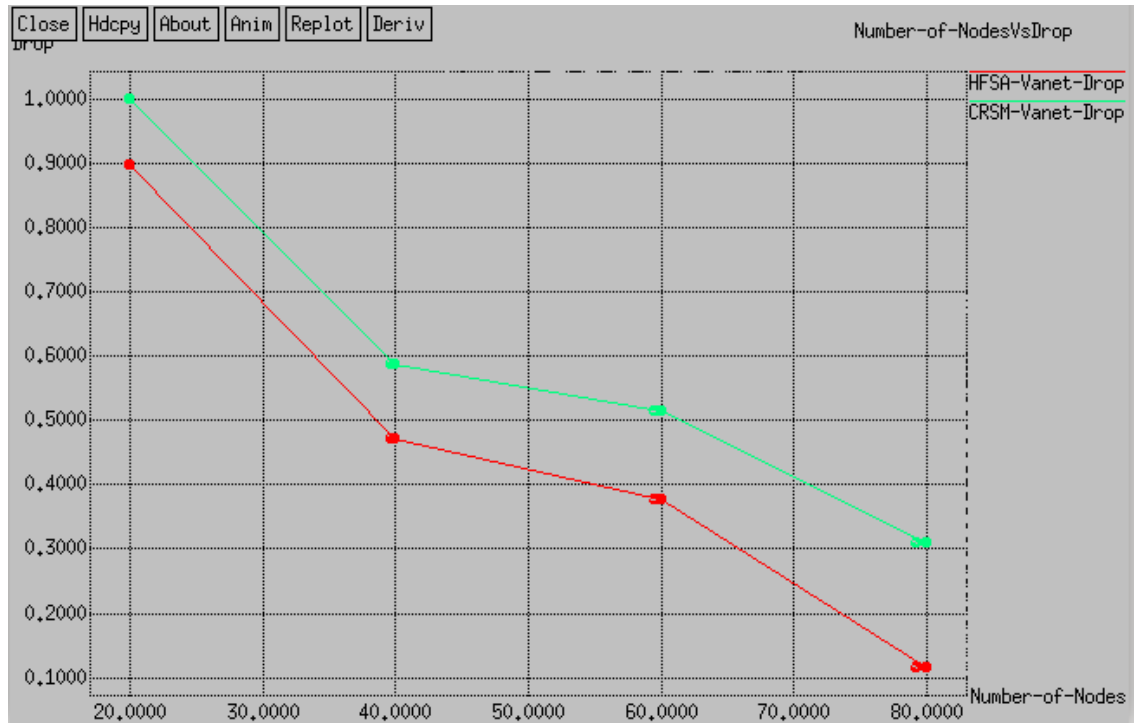


Figure 6.12: Drop plot for proposed and existing method

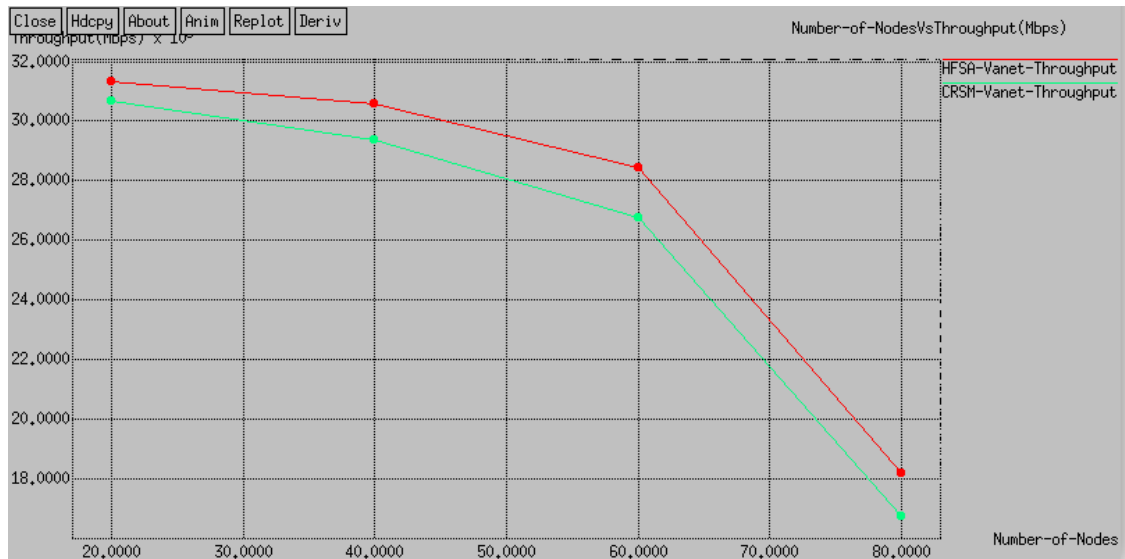


Figure 6.13: Throughput plot for proposed and existing method

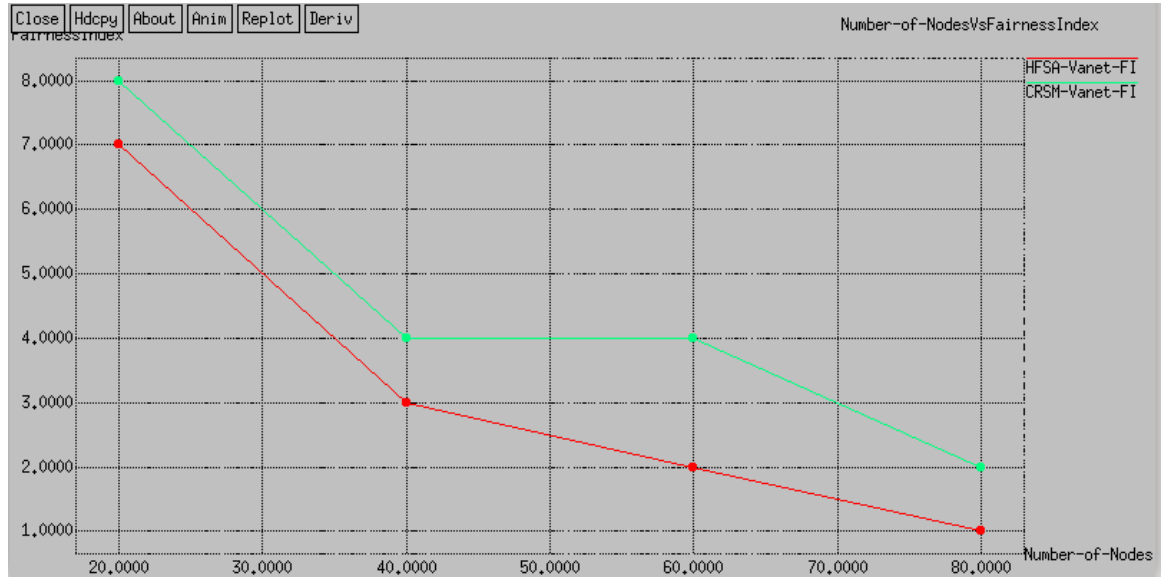


Figure 6.14: Fairness Index plot for the planned and present method

The suggested method achieves the following results in node 20th: 99J, 0.093690, and 0.897708 for energy consumption, delay value, and drop value. Additionally, the new method outperforms the old one with a Throughput of 31341, which is greater. The fairness rating for the suggested method is 7.000000, whereas the rating for the current method is 8.000000. The suggested solution achieves 47J, 9.752925, and 0.472094 for energy consumption, delay value, and drop value in node 60th. Additionally, compared to the old approach, the new one achieves a throughput of 31341. The proposed approach has a fairness value of 4.000000, whereas the suggested strategy has a score of 3.000000. The energy consumption, delay value, and drop value for the suggested method are 36J, 10.902826, and 0.376633 in the node 60th. Additionally, the proposed method obtains a Throughput of 28423 as opposed to the previous method's 26749. 2.000000 for the proposed method and 4.000000 for the current method for the fairness index. The suggested approach achieves 11J, 15.287826, and 0.116375 for energy consumption, delay value, and drop value in node 80th. The proposed strategy also achieves a Throughput of 18197 compared to the prior method. The fairness score of the suggested method is 1.000000, while the fairness value of the current approach is 2.000000. Delay, Energy Consumption, Drop, Throughput, and Fairness Index are each retrieved through a node, as shown in Figs. 6.10 to 6.14.

6.4.2. Results obtained through speed

On the basis of delay, energy use, drop, throughput, and the fairness index, the suggested technique's speed is compared to the speeds of the existing techniques. The table below provides examples of the measured values. The speed values of both current and suggested approaches are displayed in Table 6.2.

Table 6.2: Comparison of the proposed method to existing method of speed

Speed	Delay(s)		Energy consumption(Joules)		Drop(%)		Throughput(Mbps)		Fairness Index (FI)	
	HFSA-VANET[Proposed]	CRSM-VANET [164]	HFSA-VANET	CRSM-VANET	HFSA-VANET	CRSM-VANET	HFSA-VANET	CRSM-VANET	HFSA-VANET	CRSM-VANET
20	1.873793	2.47224	1980	1980	19.95416	19.96283	150	90	6	6
40	390.117	497.249781	1880	2320	18.883762	23.45486	35	26	3	4
60	654.169557	827.19374	2220	3060	22.597974	30.85639	22	16	2	3
80	1223.026093	1637.146333	880	2480	9.309993	24.8315	8	6	0	2

Below is a graphical representation that compares the speed to the delay, energy, drop, throughput, and fairness index.

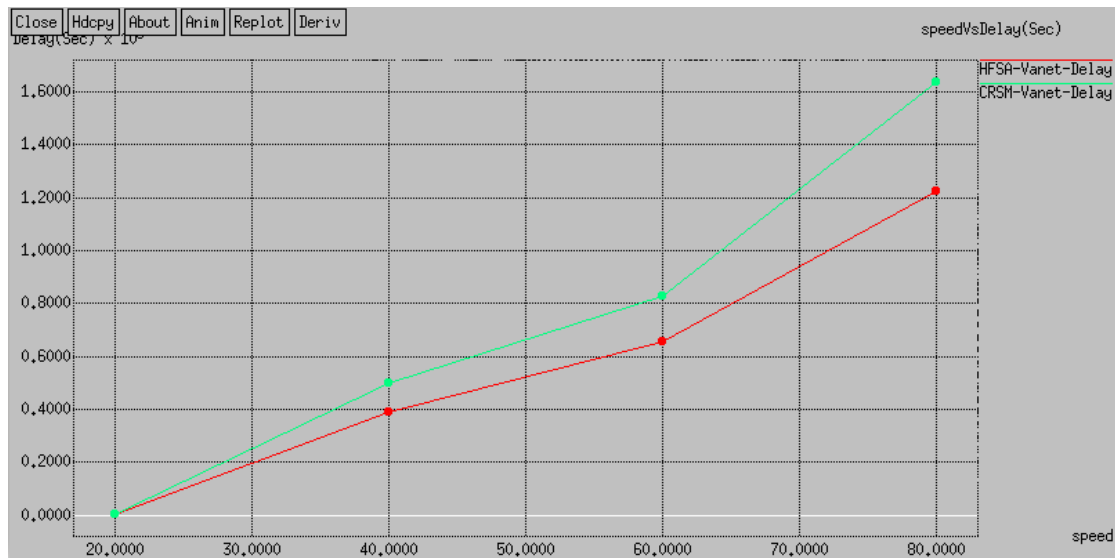


Figure 6.15: Speed Vs Delay plot for proposed and existing method

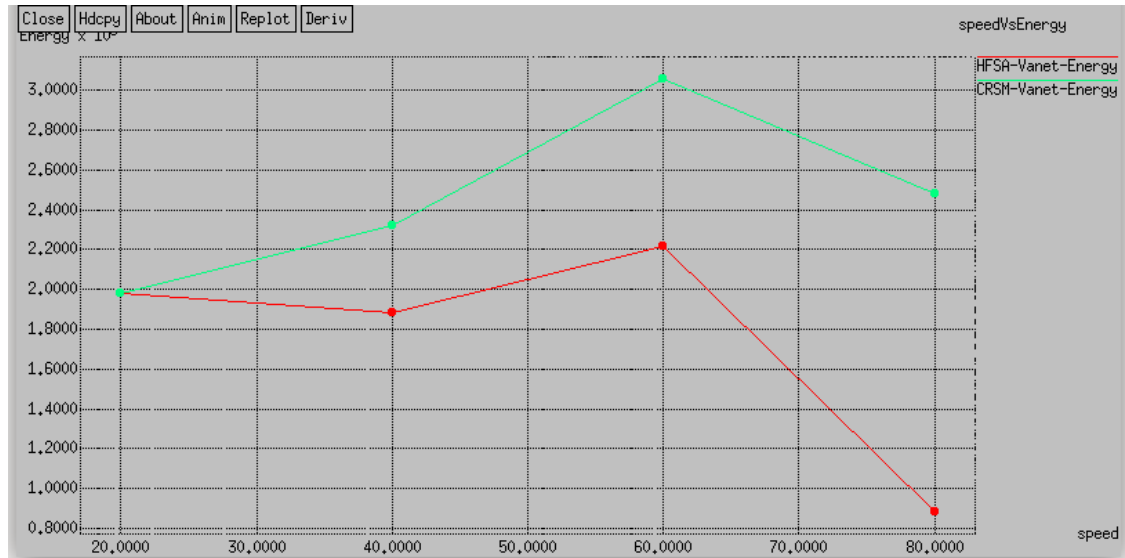


Figure 6.16: Speed Vs energy consumption plot for a proposed and existing method

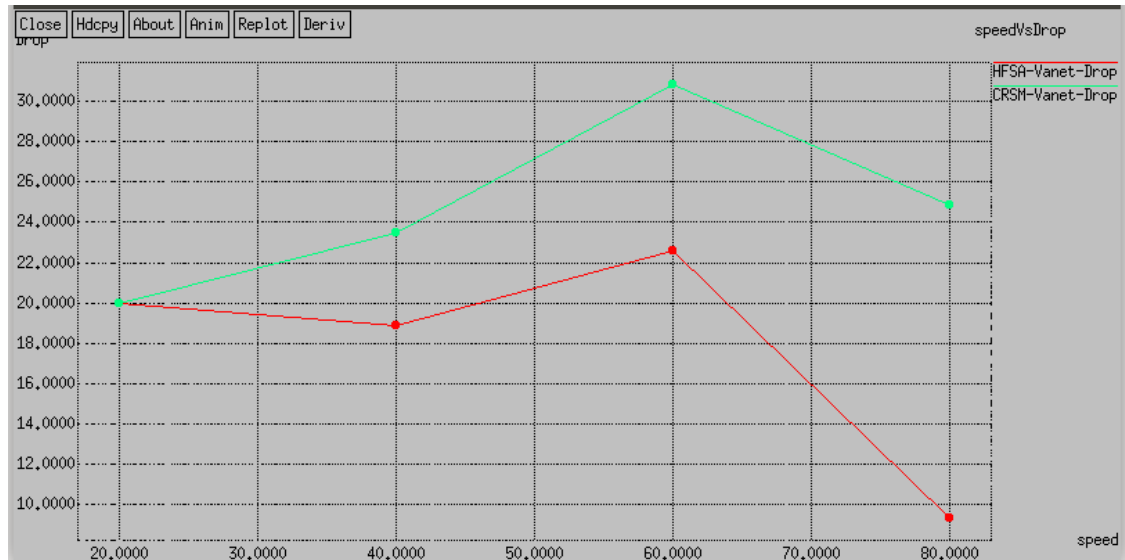


Figure 6.17: Speed Vs Drop plot for a proposed and existing method

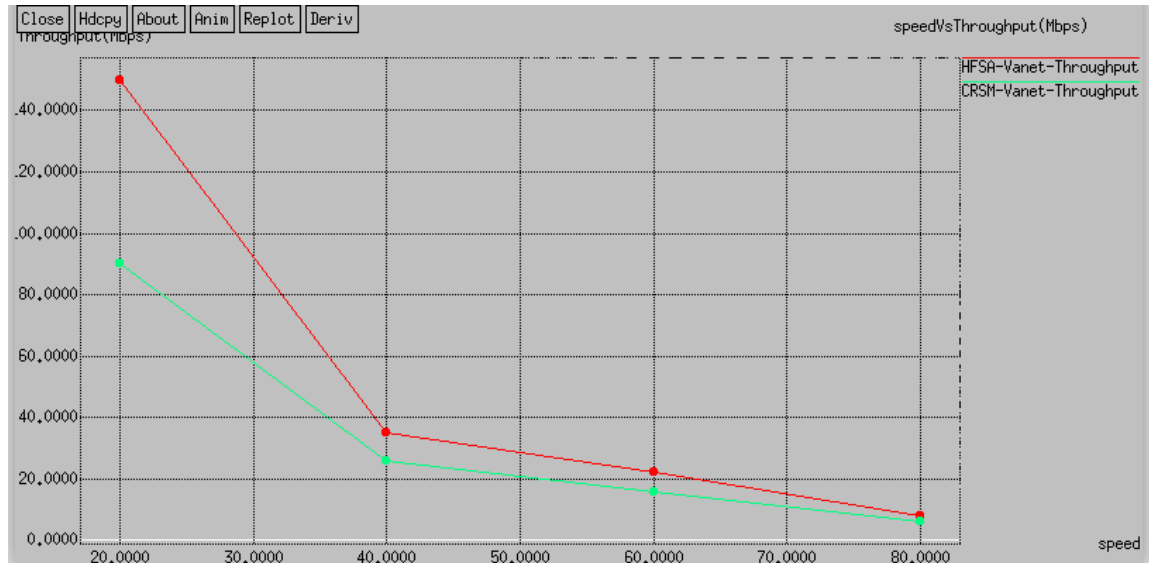


Figure 6.18: Speed Vs Throughput plot for a proposed and existing method

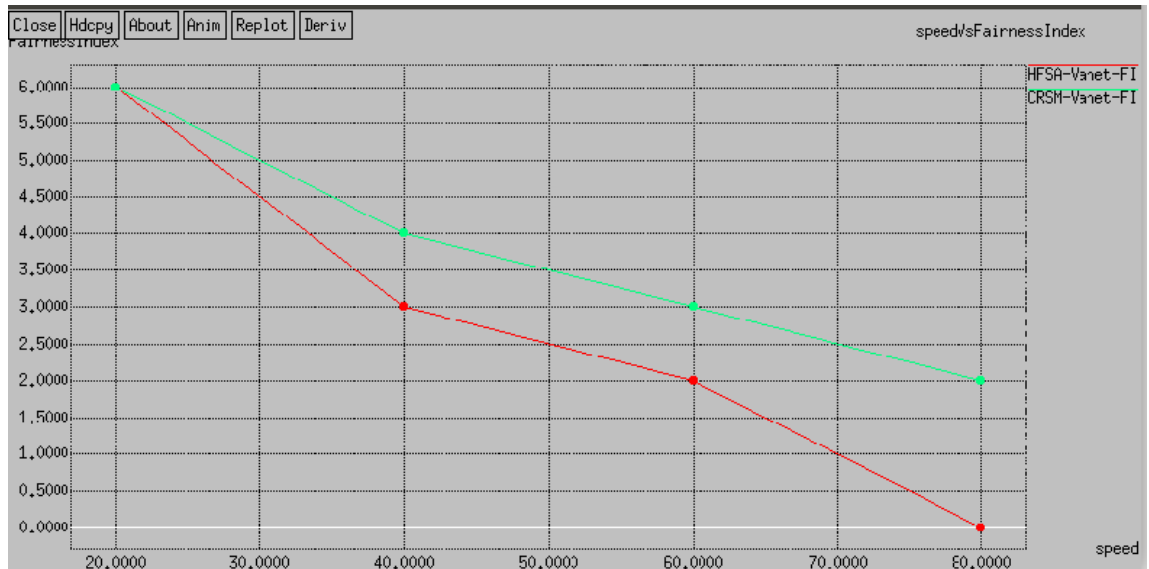


Figure 6.19: Speed Vs Fairness index plot for a proposed and existing method

The suggested method achieves 1980J, 1.873793, and 19.954160 in terms of energy consumption, delay value, and drop value at speed 20. Additionally, compared to the old approach, the new one achieves a Throughput of 150. The fairness rating for the suggested strategy is 6.000000, whereas the fairness rating for the current approach is also 6.000000. With the given method, speed 40 energy consumption, delay value, and drop value are

respectively 1880J, 390.117000, and 18.883762. Additionally, the new strategy surpasses the current strategy with a Throughput of 35. The existing method has a score of 4.000000 whereas the suggested way has a fairness value of 3.000000. The proposed method achieves 2220J, 654.169557, and 22.597974 in terms of energy consumption, delay, and drop value at speed 60. Additionally, the suggested approach results in a Throughput of 22 Vs. 16 for the current method. The fairness index of the proposed method is 2.000000, while that of the current method is 3.000000. The suggested approach achieves energy consumption, delay value, and drop value in speed 80 of 880 J, 122.32609, and 9.309993, respectively. Additionally, the new method achieves a throughput of 8, while the old method only manages a throughput of 6. The fairness score of the proposed method is 0.000000, while that of the current approach is 2.000000. Delay, Energy Consumption, Drop, Throughput, and Fairness Index are acquired by speed, respectively, and are shown in Figs. 6.15 to 6.19. The section 2 discusses the outcomes produced by the MATLAB software.

6.5. Section 2

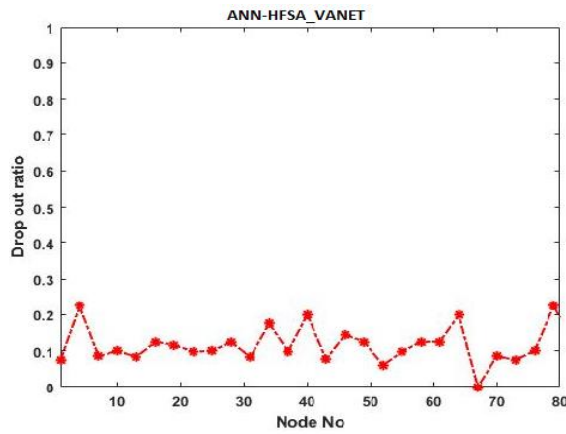
This section discusses the experimental findings that were attained using MATLAB (VERSION 2020a) to assess how well the NS2 tool performed. We also include a further parameter to guarantee the proposed model's network longevity. Therefore, it can be demonstrated that the performance is just as highly effective as the current method. Here, multiple machine learning techniques including ANN- HFSA-VANET, SVM- HFSA-VANET, NB- HFSA-VANET, and DT- HFSA-VANET are used to assess the performance of the proposed model. Thus, the results of the suggested approach may be compared and demonstrated as being more effective than any other methods now in use.

The suggested model is first assessed individually using ANN-HFSA-VANET, SVM-HFSA-VANET, NB-HFSA-VANET, and DT-HFSA-VANET. The graphical results of ANN, SVM, NB, and DT are displayed in the following figures 6.20, 21, 22, and 23, respectively. On the other hand, the suggested method is compared with a single graphical

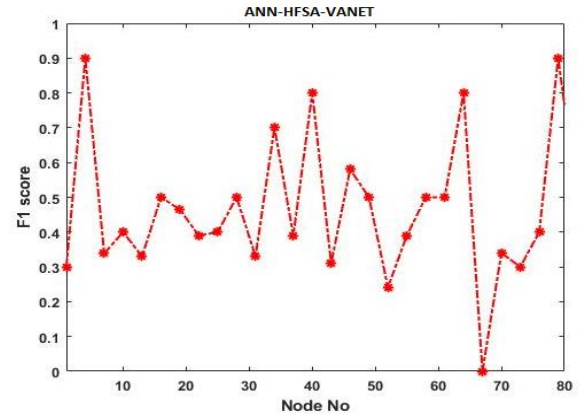
output to highlight comparability based on the aggregation of several machine learning algorithms.

6.5.1. Parameter analysis of ANN- HFSA-VANET

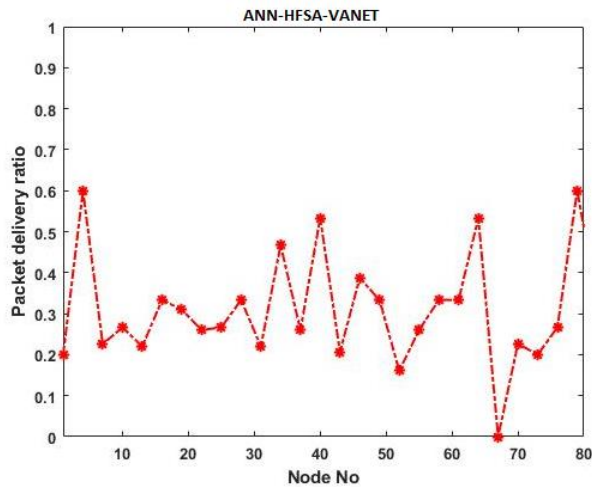
This section examines the various ANN-HFSA-VANET parameters, which are studied in the graph below (see figure 6.20).



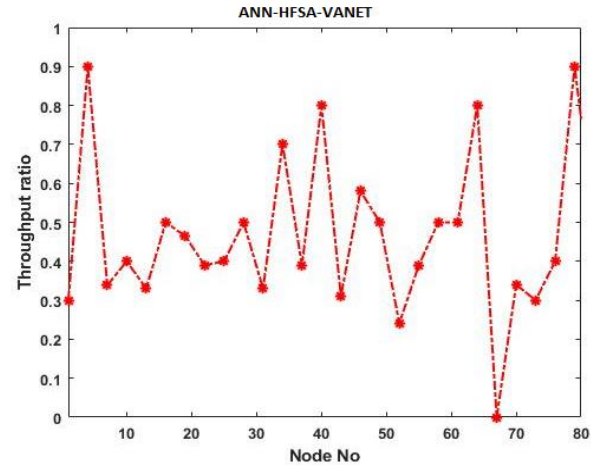
(a)



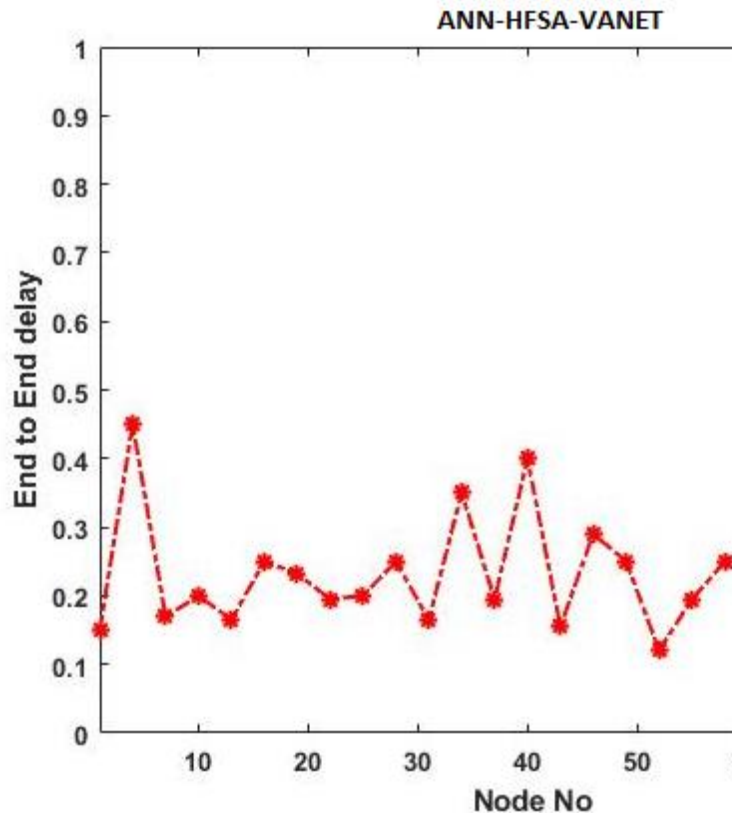
(b)



(c)



(d)



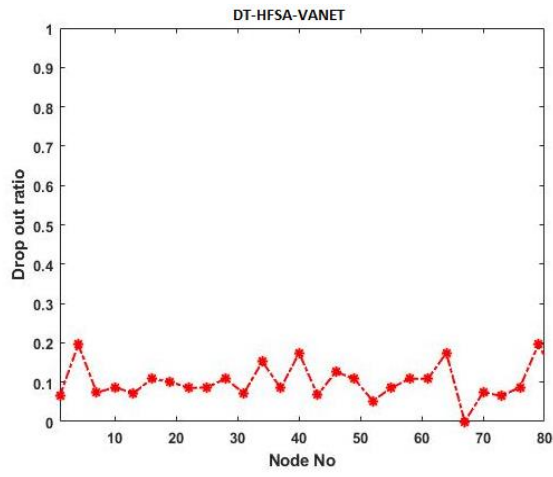
(e)

Figure 6.20: (a) Dropout ratio, (b) F1 score, (c) packet delivery ratio, (d) Throughput ratio, (e) End to end delay

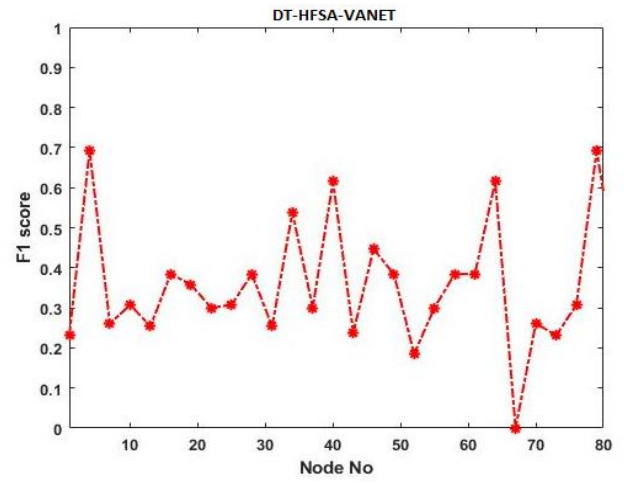
The analysis of ANN-HFSA-VANET parameters is shown in Figure 6.20. (a) displays the ANN-HFSA-drop-out VANET's ratio; (b) deals with the F1 score of the ANN-HFSA-VANET and its analysis; (c) displays the ANN-HFSA-packet VANET's delivery ratio and plots its values; (d) discusses the ANN-HFSA-throughput VANET's ratio; and (e) displays the ANN-HFSA-end-to-end VANET's delay time. The parameter values are examined, plotted in a graph, and the values are increased at the conclusion of each parameter graph.

6.5.2. Parameter analysis of Decision Tree (DT) - HFSA-VANET

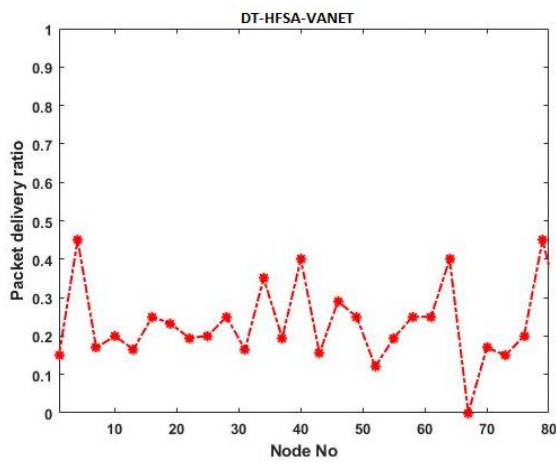
This section examines the various decision tree parameter types, which are evaluated in the graph below (see figure 6.21).



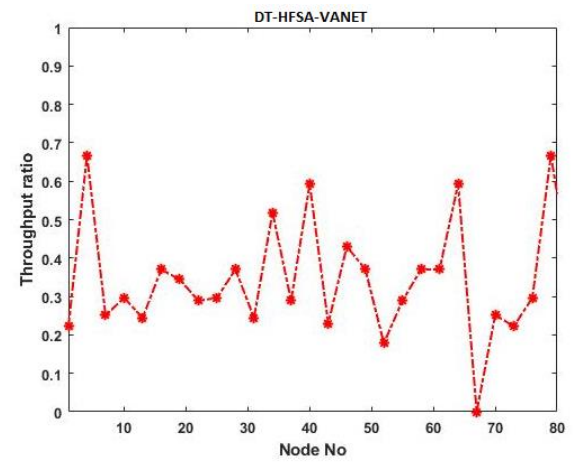
(a)



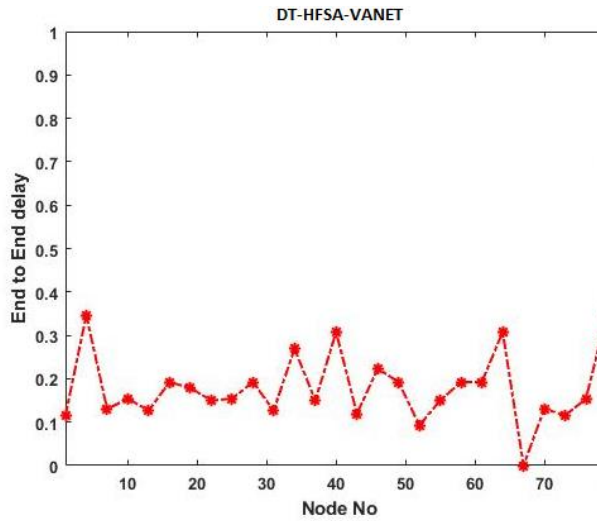
(b)



(c)



(d)



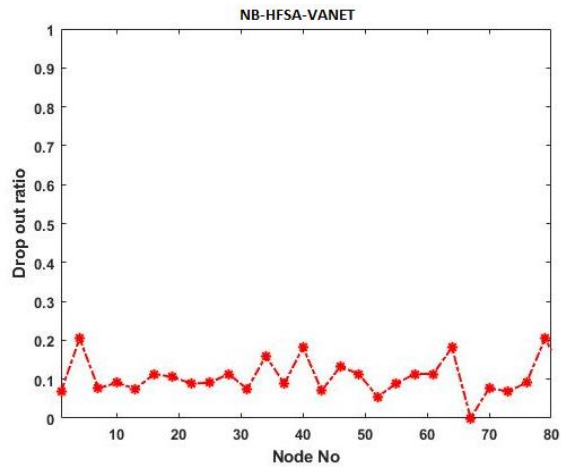
(e)

Figure 6.21: (a) Dropout ratio, (b) F1 score, (c) packet delivery ratio, (d) Throughput ratio, (e) End to end delay

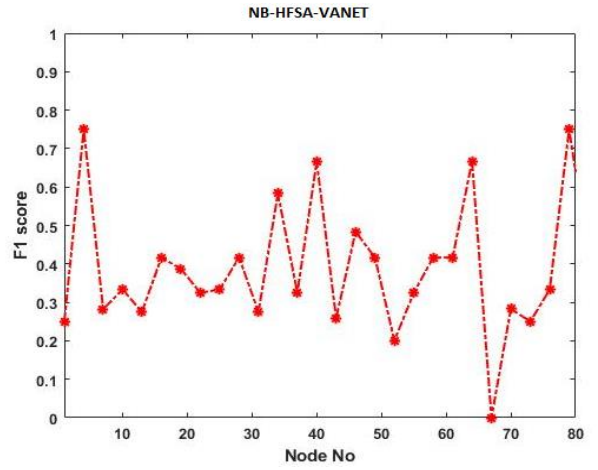
The study of the DT-HFSA-VANET parameters is shown in Figure 6.21. (A) displays the DT-HFSA-drop VANET's out ratio; (B) deals with the F1 score of the DT-HFSA-VANET and its analysis; (C) displays the DT-HFSA-packet VANET's delivery ratio and plots its values; (D) deals with the DT-HFSA-throughput VANET's ratio; and (E) deals with the DT-HFSA-end-to-end VANET's delay. The values of standard parameters are increased at the conclusion of each graph after they have been assessed and plotted.

6.5.3. Parameter analysis of Navie Bayes (NB)- HFSA-VANET

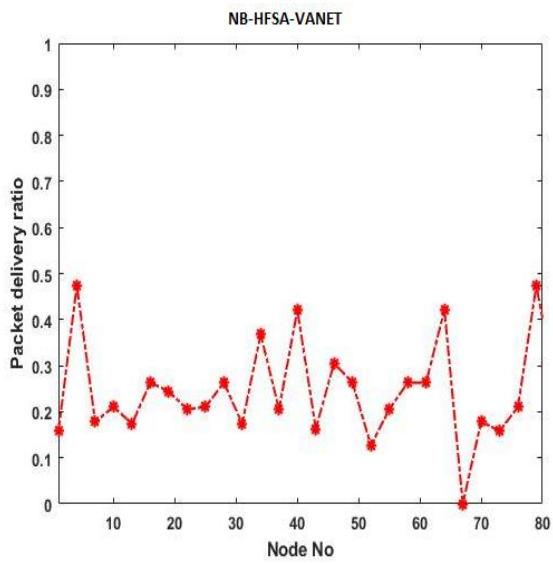
This section examines the various Navie Bayes parameter types and is evaluated in the graph below, which is seen in figure 6.22.



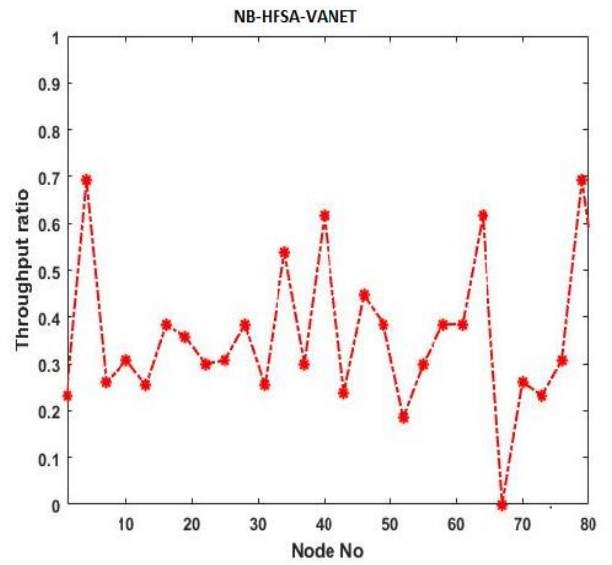
(a)



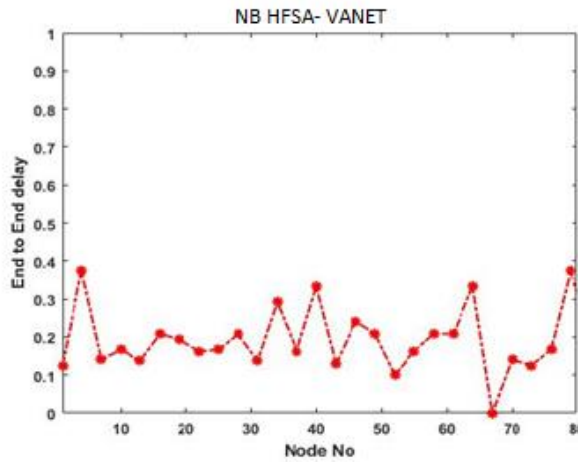
(b)



(c)



(d)



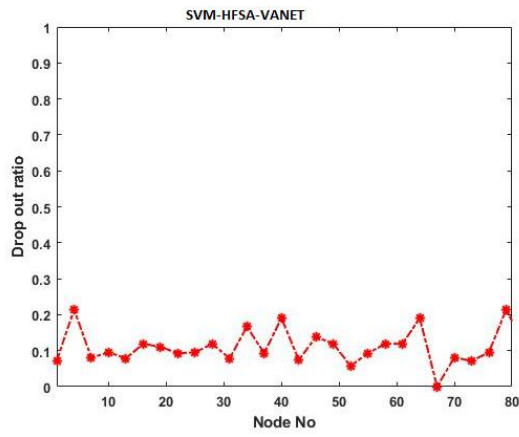
(e)

Figure 6.22:(a) Drop out ratio, (b) F1 score, (c) packet delivery ratio, (d) Through put ratio,(e) End to end delay

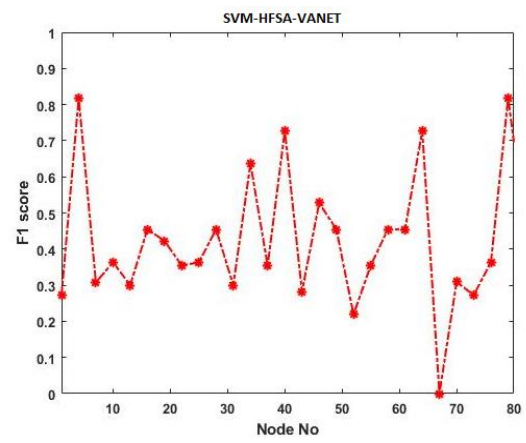
The examination of the NB-HFSA-parameters VANET's is shown in Figure 6.22. (a) displays the NB- HFSA-Dropout VANET's ratio; (b) deals with the F1 score of the network and its analysis; (c) displays the network's packet delivery ratio and plots its values; (d) addresses the throughput ratio; and (e) displays the end-to-end delay time. The parameter values are examined, plotted in a graph, and the values are increased at the conclusion of each parameter graph.

6.5.4. Parameter analysis of SVM

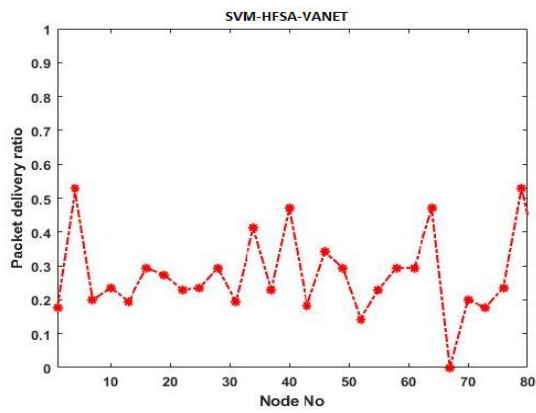
This section analyses the various SVM parameter types in the graph below, which is depicted in figure 6.23.



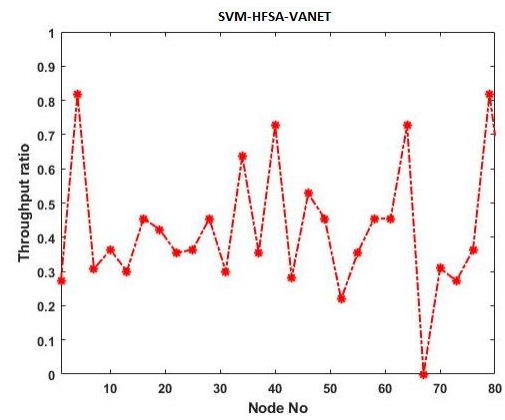
(a)



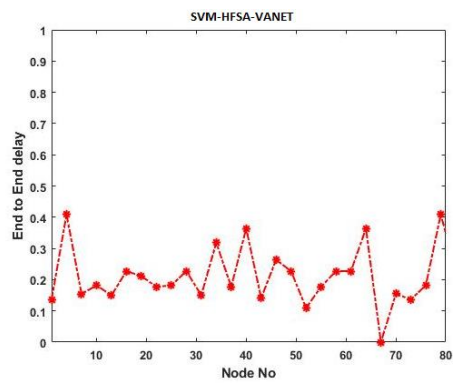
(b)



(c)



(d)



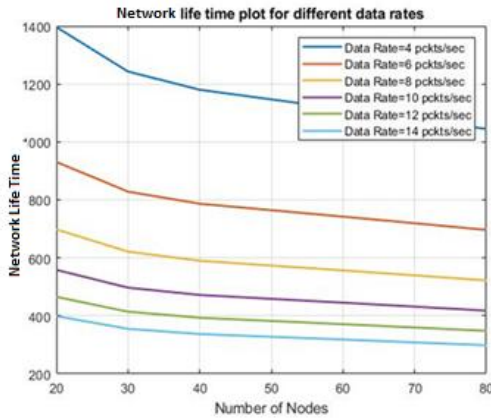
(e)

Figure 6.23:(a) Dropout ratio, (b) F1 score, (c) packet delivery ratio, (d) Through put ratio,(e) End to end delay

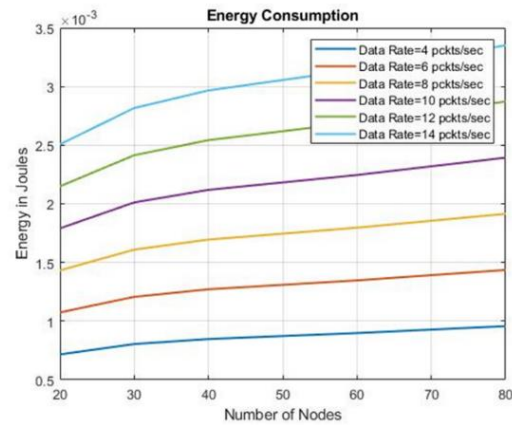
The SVM-HFSA-VANET parameter study is shown in Figure 6.23. (a) displays the SVM - HFSA-Dropout VANET's ratio; (b) deals with the F1 score of the SVM - HFSA-VANET and its analysis; (c) displays the SVM - HFSA-packet VANET's delivery ratio and plots its values; (d) discusses the SVM - HFSA-throughput VANET's ratio; and (e) displays the end-to-end delay time of the SVM - The parameter values are examined, plotted in a graph, and the values are increased at the conclusion of each parameter graph.

6.5.5. Parameters for analyzing different data types

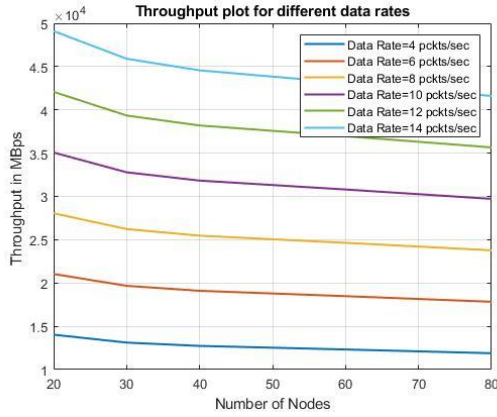
The numbers are presented in a graph in this section, which deals with the parameters of various data and their analysis.



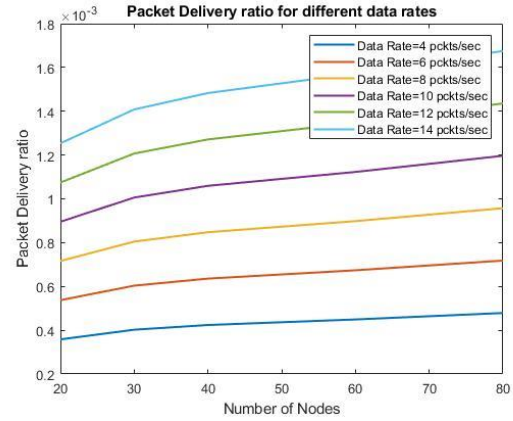
(a)



(b)



(c)



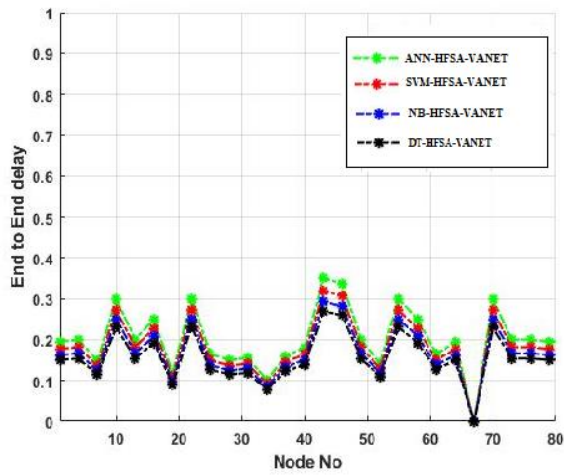
(d)

Figure 6.24 :(a) Network life time plot, (b) Energy consumption, (c) Throughput ratio, (d) Packet delivery ratio

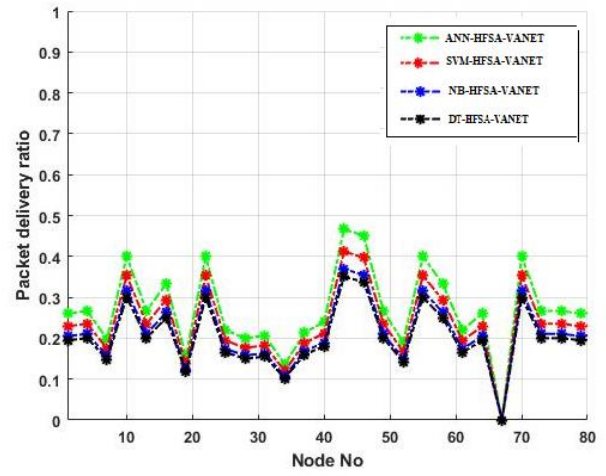
The parameter analysis value of the data kinds is reviewed and shown in a graph from figure 6.24, which displays the data ratio of the provided data values. This section deals with the following topics: (a) network time life of data kinds, (b) energy consumption of data packets consumed per second, (c) throughput ratio of data types and their performance, and (d) packet delivery ratio of various types of data performance.

6.5.6. Comparison of algorithms using parameters

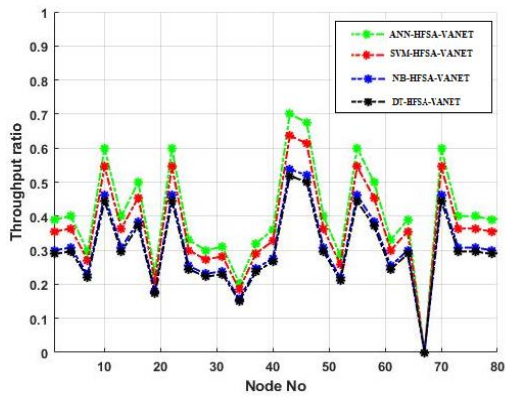
In this section, algorithms are compared using various parameters, and the values are presented on a graph. HFSA-VANET-compatible algorithms include ANN, SVM, NB, and DT.



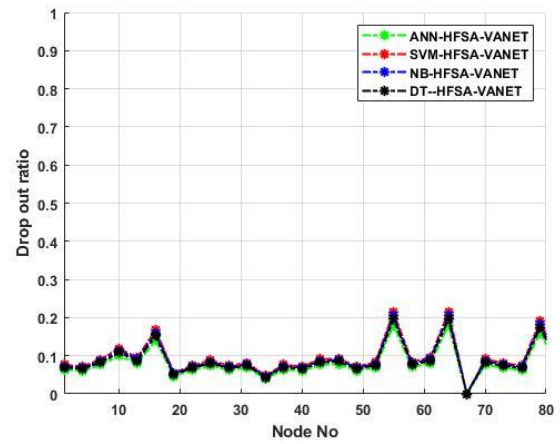
(a)



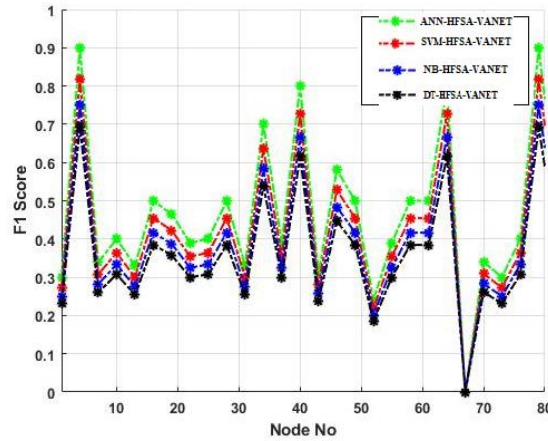
(b)



(c)



(d)



(e)

Fig 6.25: comparison of algorithms using parameters (a) End to End delay, (b) Packet delivery ratio, (c) Throughput ratio, (d) Drop out ratio, (e) F1 score

Figure 6.25 (a) discusses the end-to-end delay parameter of the existing algorithms, (b) compares the packet ratio of the existing algorithms, (c) discusses throughput ratio and algorithm performance, (d) discusses drop out ratio and algorithm performance comparison, and (e) displays the F1 score of the algorithm comparison.

6.6. Summary

By routinely inspecting each network node, the proposed ensemble with HFSA-VANET effectively maintains network stability. Artificial Fish Swarm Optimization (AFSO) and Seagull Optimization are combined with the HFSA. The performance of the AFSO, which is used for VANET enhancement, is improved by the use of the seagull optimization approach. As a result, offer very effective outcomes that are examined using an ensemble learning approach that includes ANN, SVM, DT, and Naive Bayes. The NS2 and MATLAB platforms are used for the implementation. For comparing the performance of the suggested algorithm, the HFSA-VANET is implemented in NS2 without ensemble learning and in MATLAB with ensemble learning. Moreover, the performance is analyzed based on various existing techniques. As a result, the proposed model may be demonstrated to be an approach that is far more effective than those now in use.

CHAPTER 7

CONCLUSION AND FUTURE SCOPE

7.1 Conclusion

VANET technology helps to stop the vehicle from acting maliciously in a VANET environment. Here, the proposed model was created using four separate modules.

Module 1:

In this module, a hybrid meta-heuristic technique integrated with Firefly Optimization and Whale Optimization algorithm referred as HFWOA-VANET is designed. This method examines the neighborhood vehicle data to avoid accidents and misbehavior. In this, the suggested method is compared with the present method and they are implemented in NS2 platform. The performance metrics like fairness index, energy consumption, drop, delay and throughput are analyzed. Here, the current QMM-throughput Vanet's is decreasing from 19349 to 17100 and in the introduced HFWO-Vanet, however, is achieving 20196 at Node 20th and climbed to 23402 at Node 40th, where it thereafter reached 21097. Throughput of the suggested method is more than that of the current method.

Module 2:

A congestion-free routing procedure that provides QoS standards is developed. In vehicular communication, the best routing path is selected by analyzing the effects of QoS parameters. Another scheme named Hybrid-Harris Hawks Black widow optimization-based VANET (H-HHBW-VANET) aids to increase QoS for node-to-node routing. This method is more effective than other algorithms since it generates excellent solutions. This suggested method is implemented on the NS2 platform. Here, the performances are measured based on the parameters like delay, drop, energy consumption, fairness index and throughput and they obtain minimal energy consumption with greater throughput and minimal delay. For the suggested H-HHBW-VANET, Speed 20th, delay 10.220428, drop 15.499727, energy consumption 1840, throughput 1954, and fairness index 5. Similarly, the present HFWOA-

VANET, for 20th speed, 11.220428 in delay, 19.499727 in drop, 1940 in energy consumption, 1784 in throughput, 4 in fairness index shows that the performance is far better for the suggested method. The suggested routing method is hence free of congestion, which enhances QOS performance.

Module 3:

This research project is primarily concerned with the bandwidth allocation in the VANET and identifying DDoS attacks using a machine learning-hybrid optimization technique. In this, SVM-HHO technique is used for detecting DDOS attack and their effects are reduced by using Hybrid Whale Dragonfly optimization algorithm. In this vehicular network, the stability is achieved by utilizing the forecast information for quick and reliable communication. In node 60th, the suggested methodology achieves energy consumption, delay ratio, and drop ratio of 0.35J, 50 and 14.6785 respectively. Additionally, compared to the current approach's 794 throughput, the proposed solution yields 1710 throughput. Evaluation of the estimated performance metrics like (energy consumption, latency, packet delivery ratio and throughput) shows that the performance is more effective.

Module 4:

By periodically inspecting each network node, the proposed method ensemble with HFSA-VANET is extremely successful at ensuring network stability. Seagull Optimization and Artificial Fish Swarm Optimization (AFSO) are integrated with the HFSA. As a result, highly efficient outcomes are evaluated using an ensemble learning approach that includes ANN, SVM, DT and Nave Bayes. The comparison of the algorithm shows that the suggested method achieves 1980J, 1.873793, 19.954160 in terms of energy use, delay value and drop value at speed 20. Here, the new approach accomplishes a Throughput of 150, which is higher than the old approach which has 90 for Throughput. Here, NS2 and MATLAB platforms are used for the implementation.

7.2 Future Scope:

- The VANET environment's core characteristic is authenticity. It is very important to build and allocate faith standards and to rebuild trust among vehicles in order to make the VANET environment more secure.
- The suggested hybrid metaheuristic algorithms could be used to address further significant concerns. It is noteworthy that taking the expansion of global supply chain networks into account can make the suggested hybrid algorithms more useful.
- The performance and the computation speed of the recommended optimization algorithm in routing protocol has to be enhanced and evaluated by resolving the better models in multi-objective issues.
- Focus must be placed on offering multi-constrained QoS routing and balancing trade-offs between them for a variety of QoS requirements in various scenarios.
- Utilizing various machine learning models will improve plausibility checks incorporated into the feature vector to improve performance in terms of recall and precision.
- Several performance metrics, including throughput, delay, drop, network lifetime, and energy efficiency are used to analyze the performance. But to improve the detection capacity additional QOS factors must be considered.
- The recent development of novel integrated architectures and access methods (such as fog, edge, and so on), the computational load of suggested algorithms can be eased by moving some of the tasks to external computing and storage servers situated at the edge, fog, or cloud.
- Depending on the congestion resolution algorithm, the potential relay nodes wait the longest before retransmission. This method causes a significant delay, especially when there is substantial mobility. So, it needs to be conquered.

List of Publications

- [1] Marwah, G.P.K., Jain, A. A hybrid optimization with ensemble learning to ensure VANET network stability based on performance analysis. *Sci Rep* 12, 10287 (2022). <https://doi.org/10.1038/s41598-022-14255-1>
- [2] Gaganpreet Kour Marwah and Anuj Jain. Congestion-free routing based on a hybrid meta-heuristic algorithm to provide an effective routing protocol by analyzing the significant impacts of QoS parameters in a dynamic VANET environment. 2022 *J. Phys.: Conf. Ser.* 2251 012009
- [3] G. Marwah and A. Jain, "Road Steering system with several metrics (RSSSM): A novel technique for a Smart Vehicular Network to control congestion," in *2021 International Conference on Computing Sciences (ICCS)*, Phagwara, India, 2021 pp. 112-117. doi: 10.1109/ICCS54944.2021.00030
- [4] Gagan preet Kour Marwah and Anuj Jain, "AN ALGORITHM TO DETECT MALICIOUS ACTIVITY IN DYNAMIC VANET ENVIRONMENT, Springer. [Accepted]
- [5] Gagan preet Kour Marwah and Anuj Jain, "Vehicular Adhoc Networks: A Review", Springer. [Accepted]
- [6] Gagan preet Kour Marwah and Anuj Jain, "A HYBRID META-HEURISTIC ALGORITHM TO DETECT MALICIOUS ACTIVITY BASED ON DYNAMIC VANET ENVIRONMENTAL INFORMATION", *Vehicular Communications* [Under Review]
- [7] Gagan preet Kour Marwah and Anuj Jain, "A ROBUST COMMUNICATION BASED ON AN IMPROVED MACHINE LEARNING WITH HYBRID TECHNIQUE IN VANET", *International Journal of Machine Learning and Cybernetics* [Under Review]
- [8] Gagan preet Kour Marwah and Anuj Jain, "A hybrid metaheuristic based enhanced approach to achieve network stability based on ensemble approach with comparative performance", *International Journal of Pattern recognition and Artificial Intelligence* [Under Review]
- [9] Gagan preet Kour Marwah , Anuj Jain, Praveen Malik and Manwinder Singh, "An Improved Machine Learning with Hybrid Technique in Vanet for Robust Communication. *Sensors* [Under Review]

References

1. Fatemidokht, H., Rafsanjani, M.K., Gupta, B.B. and Hsu, C.H., 2021. Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular ad hoc networks in intelligent transportation systems. *IEEE Transactions on Intelligent Transportation Systems*, 22(7), pp.4757-4769.
2. Mirsadeghi, F., Rafsanjani, M.K. and Gupta, B.B., 2021. A trust infrastructure-based authentication method for clustered vehicular ad hoc networks. *Peer-to-Peer Networking and Applications*, 14(4), pp.2537-2553.
3. Ali, I., Lawrence, T., Omala, A.A. and Li, F., 2020. An efficient hybrid signcryption scheme with conditional privacy-preservation for heterogeneous vehicular communication in VANETs. *IEEE Transactions on Vehicular Technology*, 69(10), pp.11266-11280.
4. Bayat, M., Pournaghi, M., Rahimi, M. and Barmshoory, M., 2020. NERA: A new and efficient RSU based authentication scheme for VANETs. *Wireless networks*, 26(5), pp.3083-3098.
5. Gao, H., Liu, C., Li, Y. and Yang, X., 2020. V2VR: reliable hybrid-network-oriented V2V data transmission and routing considering RSUs and connectivity probability. *IEEE Transactions on Intelligent Transportation Systems*, 22(6), pp.3533-3546.
6. Dutta, A.K., Elhoseny, M., Dahiya, V. and Shankar, K., 2020. An efficient hierarchical clustering protocol for multihop Internet of vehicles communication. *Transactions on Emerging Telecommunications Technologies*, 31(5), p.e3690.
7. Ali, E.S., Hasan, M.K., Hassan, R., Saeed, R.A., Hassan, M.B., Islam, S., Nafi, N.S. and Bevinakoppa, S., 2021. Machine learning technologies for secure vehicular communication in internet of vehicles: recent advances and applications. *Security and Communication Networks*, 2021.
8. Lee, M. and Atkison, T., 2021. Vanet applications: Past, present, and future. *Vehicular Communications*, 28, p.100310.

9. Khelifi, H., Luo, S., Nour, B., Moun gla, H., Faheem, Y., Hussain, R. and Ksentini, A., 2019. Named data networking in vehicular ad hoc networks: State-of-the-art and challenges. *IEEE Communications Surveys & Tutorials*, 22(1), pp.320-351.
10. Mundhe, P., Yadav, V.K., Singh, A., Verma, S. and Venkatesan, S., 2020. Ring signature-based conditional privacy-preserving authentication in VANETs. *Wireless Personal Communications*, 114(1), pp.853-881.
11. Oche, M., Tambuwal, A.B., Chemebe, C., Noor, R.M. and Distefano, S., 2020. VANETs QoS-based routing protocols based on multi-constrained ability to support ITS infotainment services. *Wireless Networks*, 26(3), pp.1685-1715.
12. Bamhdi, A.M., 2020. Efficient dynamic-power AODV routing protocol based on node density. *Computer Standards & Interfaces*, 70, p.103406.
13. Gasmi, R., Aliouat, M. and Seba, H., 2020. A stable link based zone routing protocol (SL-ZRP) for internet of vehicles environment. *Wireless Personal Communications*, 112(2), pp.1045-1060.
14. Usha, M. and Ramakrishnan, B., 2019. An enhanced MPR OLSR protocol for efficient node selection process in cognitive radio based VANET. *Wireless Personal Communications*, 106(2), pp.763-787.
15. Raissi, K. and Gouissem, B.B., 2018. Comparative Study of Ad Hoc Routing Protocols in Vehicular Ad-Hoc Networks for Smart City. *International Journal of Information and Communication Engineering*, 12(3), pp.176-181.
16. Raissi, K. and Ben Gouissem, B., 2021. Hybrid communication architecture in VANETs via named data network. *International Journal of Communication Systems*, 34(11), p.e4848.
17. Ur Rehman, M., Ahmed, S., Ullah Khan, S., Begum, S. and Ahmed, S.H., 2018. Performance and execution evaluation of VANETs routing protocols in different scenarios. *EAI Endorsed Transactions on Energy Web*, 5(17).
18. Singh, V. and Saini, G.L., 2018. DTN-enabled routing protocols and their potential influence on vehicular ad hoc networks. In *Soft Computing: Theories and Applications* (pp. 367-375). Springer, Singapore.

19. Guleria, A. and Singh, K., 2017. Position based adaptive routing for VANETs. *International Journal of Computer Networks & Communications (IJCNC)* Vol, 9.
20. Jayeola, A.O. and Rotimi, O.J., Most Reliable Position Based Routing Protocol in Vehicular Ad hoc Network (VANET).
21. Srivastava, A., Prakash, A. and Tripathi, R., 2020. Location based routing protocols in VANET: Issues and existing solutions. *Vehicular Communications*, 23, p.100231.
22. Senouci, O., Aliouat, Z. and Harous, S., 2019. MCA-V2I: A multi-hop clustering approach over vehicle-to-internet communication for improving VANETs performances. *Future Generation Computer Systems*, 96, pp.309-323.
23. Kühlmorgen, S., Lu, H., Festag, A., Kenney, J., Gensheim, S. and Fettweis, G., 2019. Evaluation of congestion-enabled forwarding with mixed data traffic in vehicular communications. *IEEE Transactions on Intelligent Transportation Systems*, 21(1), pp.233-247.
24. Cui, J., Wei, L., Zhang, J., Xu, Y. and Zhong, H., 2018. An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, 20(5), pp.1621-1632.
25. Obaidat, M., Khodjaeva, M., Holst, J. and Ben Zid, M., 2020. Security and privacy challenges in vehicular ad hoc networks. In *Connected Vehicles in the Internet of Things* (pp. 223-251). Springer, Cham.
26. Abassi, R., 2019. VANET security and forensics: Challenges and opportunities. *Wiley Interdisciplinary Reviews: Forensic Science*, 1(2), p.e1324.
27. Gupta, R., Tanwar, S., Tyagi, S. and Kumar, N., 2020. Machine learning models for secure data analytics: A taxonomy and threat model. *Computer Communications*, 153, pp.406-440.
28. AlFarraj, O., Tolba, A., Alkhalaf, S. and AlZubi, A., 2019. Neighbor predictive adaptive handoff algorithm for improving mobility management in VANETs. *Computer Networks*, 151, pp.224-231.

29. Das, D. and Misra, R., 2018. Improvised dynamic network connectivity model for Vehicular Ad-Hoc Networks (VANETs). *Journal of Network and Computer Applications*, 122, pp.107-114.
30. Ahmed, H., Pierre, S. and Quintero, A., 2018. A cooperative road topology-based handoff management scheme. *IEEE Transactions on Vehicular Technology*, 68(4), pp.3154-3162.
31. Nguyen, V., Pham, C., Oo, T.Z., Tran, N.H., Huh, E.N. and Hong, C.S., 2019. MAC protocols with dynamic interval schemes for VANETs. *Vehicular Communications*, 15, pp.40-62.
32. Gupta, N., Jain, A., Vaisla, K.S., Kumar, A. and Kumar, R., 2021. Performance analysis of DSDV and OLSR wireless sensor network routing protocols using FPGA hardware and machine learning. *Multimedia Tools and Applications*, 80(14), pp.22301-22319.
33. Nama, M., Nath, A., Bechra, N., Bhatia, J., Tanwar, S., Chaturvedi, M. and Sadoun, B., 2021. Machine learning-based traffic scheduling techniques for intelligent transportation system: opportunities and challenges. *International Journal of Communication Systems*, 34(9), p.e4814.
34. Yao, L., Wang, J., Wang, X., Chen, A. and Wang, Y., 2017. V2X routing in a VANET based on the hidden Markov model. *IEEE Transactions on Intelligent Transportation Systems*, 19(3), pp.889-899.
35. Guidoni, D.L., Maia, G., Souza, F.S., Villas, L.A. and Loureiro, A.A., 2020. Vehicular traffic management based on traffic engineering for vehicular ad hoc networks. *IEEE Access*, 8, pp.45167-45183.
36. Usama, M., Qadir, J., Raza, A., Arif, H., Yau, K.L.A., Elkhatib, Y., Hussain, A. and Al-Fuqaha, A., 2019. Unsupervised machine learning for networking: Techniques, applications and research challenges. *IEEE access*, 7, pp.65579-65615.
37. Ibrar, M., Akbar, A., Jan, R., Jan, M.A., Wang, L., Song, H. and Shah, N., 2020. Artnet: Ai-based resource allocation and task offloading in a reconfigurable internet of vehicular networks. *IEEE Transactions on Network Science and Engineering*.

38. Bangui, H., Ge, M. and Buhnova, B., 2022. A hybrid machine learning model for intrusion detection in vanet. *Computing*, 104(3), pp.503-531.
39. Zadobrischi, E., Dimian, M. and Negru, M., 2021. The utility of DSRC and V2X in road safety applications and intelligent parking: similarities, differences, and the future of vehicular communication. *Sensors*, 21(21), p.7237.
40. Li, W., Song, W., Lu, Q. and Yue, C., 2020. Reliable congestion control mechanism for safety applications in urban VANETs. *Ad Hoc Networks*, 98, p.102033.
41. Jayachandran, S., 2021. Transmission Data Rate Control Based Mechanism for Congestion Control in Vehicular Ad Hoc Networks (VANET) (Doctoral dissertation, University of Windsor (Canada)).
42. Liu, J., Bai, F., Weng, H., Li, S., Cui, X. and Zhang, Y., 2020. A routing algorithm based on real-time information traffic in sparse environment for VANETs. *Sensors*, 20(24), p.7018.
43. Abuashour, A. and Kadoch, M., 2017. Performance improvement of cluster-based routing protocol in VANET. *Ieee access*, 5, pp.15354-15371.
44. Dinh, N.T. and Kim, Y., 2017. Information-centric dissemination protocol for safety information in vehicular ad-hoc networks. *Wireless Networks*, 23(5), pp.1359-1371.
45. Zeng, F., Zhang, R., Cheng, X. and Yang, L., 2017. Channel prediction based scheduling for data dissemination in VANETs. *IEEE Communications Letters*, 21(6), pp.1409-1412.
46. Jaballah, W.B., Conti, M. and Lal, C., 2020. Security and design requirements for software-defined VANETs. *Computer Networks*, 169, p.107099.
47. Li, S., Liu, Y., Wang, J. and Sun, Z., 2020. SCMAC: A slotted-contention-based media access control protocol for cooperative safety in VANETs. *IEEE Internet of Things Journal*, 7(5), pp.3812-3821.
48. Khatri, S., Vachhani, H., Shah, S., Bhatia, J., Chaturvedi, M., Tanwar, S. and Kumar, N., 2021. Machine learning models and techniques for VANET based traffic management: Implementation issues and challenges. *Peer-to-Peer Networking and Applications*, 14(3), pp.1778-1805.

49. Cao, Y., Zhang, H., Fang, Y. and Yuan, D., 2020. An adaptive high-throughput multichannel MAC protocol for VANETs. *IEEE Internet of Things Journal*, 7(9), pp.8249-8262.
50. Majumder, S., Mathur, A. and Javaid, A.Y., 2019, June. A study on recent applications of blockchain technology in vehicular adhoc network (VANET). In *National Cyber Summit* (pp. 293-308). Springer, Cham.
51. Binu, G.S. and Shajimohan, B., 2020. A novel heuristic based energy efficient routing strategy in wireless sensor network. *Peer-to-Peer Networking and Applications*, 13(6), pp.1853-1871.
52. Hasan, M.Z., Al-Turjman, F. and Al-Rizzo, H., 2018. Analysis of cross-layer design of quality-of-service forward geographic wireless sensor network routing strategies in green internet of things. *IEEE Access*, 6, pp.20371-20389.
53. Sampathkumar, A., Mulerikkal, J. and Sivaram, M., 2020. Glowworm swarm optimization for effectual load balancing and routing strategies in wireless sensor networks. *Wireless Networks*, 26(6), pp.4227-4238.
54. Xu, C., Xiong, Z., Zhao, G. and Yu, S., 2019. An energy-efficient region source routing protocol for lifetime maximization in WSN. *IEEE Access*, 7, pp.135277-135289.
55. Arjunan, S. and Sujatha, P., 2018. Lifetime maximization of wireless sensor network using fuzzy based unequal clustering and ACO based routing hybrid protocol. *Applied Intelligence*, 48(8), pp.2229-2246.
56. Lin, D., Min, W. and Xu, J., 2020. An energy-saving routing integrated economic theory with compressive sensing to extend the lifespan of WSNs. *IEEE Internet of Things Journal*, 7(8), pp.7636-7647.
57. Peixoto, M.L.M., Maia, A.H.O., Mota, E., Rangel, E., Costa, D.G., Turgut, D. and Villas, L.A., 2021. A traffic data clustering framework based on fog computing for vanets. *Vehicular Communications*, 31, p.100370.

58. Wang, Q., Lin, D., Yang, P. and Zhang, Z., 2019. An energy-efficient compressive sensing-based clustering routing protocol for WSNs. *IEEE Sensors Journal*, 19(10), pp.3950-3960.
59. Micheletti, M., Mostarda, L. and Navarra, A., 2019. CER-CH: combining election and routing amongst cluster heads in heterogeneous WSNs. *IEEE Access*, 7, pp.125481-125493.
60. Chalapathi, G.S.S., Chamola, V., Gurunarayanan, S. and Sikdar, B., 2019. E-SATS: An efficient and simple time synchronization protocol for cluster-based wireless sensor networks. *IEEE Sensors Journal*, 19(21), pp.10144-10156.
61. Khan, A., Ali, I., Ghani, A., Khan, N., Alsaqer, M., Rahman, A.U. and Mahmood, H., 2018. Routing protocols for underwater wireless sensor networks: Taxonomy, research challenges, routing strategies and future directions. *Sensors*, 18(5), p.1619.
62. Amgoth, T. and Jana, P.K., 2015. Energy-aware routing algorithm for wireless sensor networks. *Computers & Electrical Engineering*, 41, pp.357-367.
63. Attiah, A., Amjad, M.F., Chatterjee, M. and Zou, C., 2018. An evolutionary routing game for energy balance in Wireless Sensor Networks. *Computer Networks*, 138, pp.31-43.
64. Xu, Z., Chen, L., Liu, T., Cao, L. and Chen, C., 2015. Balancing energy consumption with hybrid clustering and routing strategy in wireless sensor networks. *Sensors*, 15(10), pp.26583-26605.
65. Anisi, M.H., Abdul-Salaam, G., Idris, M., Idna, Y., Wahab, A.W.A. and Ahmedy, I., 2017. Energy harvesting and battery power based routing in wireless sensor networks. *Wireless Networks*, 23(1), pp.249-266.
66. Sun, B. and Li, D., 2017. A comprehensive trust-aware routing protocol with multi-attributes for WSNs. *IEEE Access*, 6, pp.4725-4741.
67. He, Y., Han, G., Wang, H., Ansere, J.A. and Zhang, W., 2019. A sector-based random routing scheme for protecting the source location privacy in WSNs for the Internet of Things. *Future Generation Computer Systems*, 96, pp.438-448.

68. Chen, W., Zhang, M., Hu, G., Tang, X. and Sangaiah, A.K., 2017. Constrained random routing mechanism for source privacy protection in WSNs. *IEEE Access*, 5, pp.23171-23181.
69. Thangaramya, K., Kulothungan, K., Indira Gandhi, S., Selvi, M., Santhosh Kumar, S.V.N. and Arputharaj, K., 2020. Intelligent fuzzy rule-based approach with outlier detection for secured routing in WSN. *Soft Computing*, 24(21), pp.16483-16497.
70. Zeng, B. and Dong, Y., 2016. An improved harmony search based energy-efficient routing algorithm for wireless sensor networks. *Applied Soft Computing*, 41, pp.135-147.
71. Haouari, N., Moussaoui, S. and Senouci, S.M., 2018, May. Application reliability analysis of density-aware congestion control in VANETs. In 2018 IEEE (pp. 1-6). IEEE.
72. Lyu, F., Cheng, N., Zhou, H., Xu, W., Shi, W., Chen, J. and Li, M., 2018. DBCC: Leveraging link perception for distributed beacon congestion control in VANETs. *IEEE Internet of Things Journal*, 5(6), pp.4237-4249.
73. Rath, M., Pati, B. and Pattanayak, B.K., 2019. Mobile agent-based improved traffic control system in VANET. In *Integrated Intelligent Computing, Communication and Security* (pp. 261-269). Springer, Singapore.
74. Lyamin, N., Bellalta, B. and Vinel, A., 2020. Age-of-information-aware decentralized congestion control in vanets. *IEEE Networking Letters*, 2(1), pp.33-37.
75. Paranjothi, A., Khan, M.S., Patan, R., Parizi, R.M. and Atiquzzaman, M., 2020. VANETomo: A congestion identification and control scheme in connected vehicles using network tomography. *Computer Communications*, 151, pp.275-289.
76. Feukeu, E.A. and Zuva, T., 2020. Dynamic broadcast storm mitigation approach for VANETs. *Future Generation Computer Systems*, 107, pp.1097-1104.
77. Rao, A.N., Naik, R. and Devi, N., 2021. On Maximizing the Coverage and Network Lifetime in Wireless Sensor Networks Through Multi-Objective Metaheuristics. *Journal of The Institution of Engineers (India): Series B*, 102(1), pp.111-122.

78. Goudarzi, F. and Asgari, H., 2018. Non-cooperative beacon power control for VANETs. *IEEE Transactions on Intelligent Transportation Systems*, 20(2), pp.777-782.
79. Ullah, A., Yaqoob, S., Imran, M. and Ning, H., 2018. Emergency message dissemination schemes based on congestion avoidance in VANET and vehicular FoG computing. *IEEE Access*, 7, pp.1570-1585.
80. Toutouh, J. and Alba, E., 2018. A swarm algorithm for collaborative traffic in vehicular networks. *Vehicular Communications*, 12, pp.127-137.
81. Ravi, B. and Thangaraj, J., 2021. Stochastic traffic flow modeling for multi-hop cooperative data dissemination in VANETs. *Physical Communication*, 46, p.101290.
82. Lyamin, N., Kleyko, D., Delooz, Q. and Vinel, A., 2018. AI-based malicious network traffic detection in VANETs. *IEEE Network*, 32(6), pp.15-21.
83. Sangaiah, A.K., Ramamoorthi, J.S., Rodrigues, J.J., Rahman, M.A., Muhammad, G. and Alrashoud, M., 2020. LACCVoV: linear adaptive congestion control with optimization of data dissemination model in vehicle-to-vehicle communication. *IEEE Transactions on Intelligent Transportation Systems*, 22(8), pp.5319-5328.
84. Garg, S., Singh, A., Kaur, K., Aujla, G.S., Batra, S., Kumar, N. and Obaidat, M.S., 2019. Edge computing-based security framework for big data analytics in VANETs. *IEEE Network*, 33(2), pp.72-81.
85. Karpagalakshmi, R.C., Vijayalakshmi, P., Gowsic, K. and Rathi, R., 2021. An effective traffic management system using connected dominating set forwarding (CDSF) framework for reducing traffic congestion in high density vanets. *Wireless Personal Communications*, 119(3), pp.2725-2754.
86. Taherkhani, N. and Pierre, S., 2016. Centralized and localized data congestion control strategy for vehicular ad hoc networks using a machine learning clustering algorithm. *IEEE Transactions on Intelligent Transportation Systems*, 17(11), pp.3275-3285.
87. Taherkhani, N. and Pierre, S., 2015. Improving dynamic and distributed congestion control in vehicular ad hoc networks. *Ad Hoc Networks*, 33, pp.112-125.

88. Amer, H.M., Tsotskas, C., Hawes, M., Franco, P. and Mihaylova, L., 2017, October. A game theory approach for congestion control in vehicular ad hoc networks. In *2017 Sensor Data Fusion: Trends, Solutions, Applications (SDF)* (pp. 1-6). IEEE.
89. Gómez, A.A. and Mecklenbräuker, C.F., 2016. Dependability of decentralized congestion control for varying VANET density. *IEEE Transactions on Vehicular Technology*, 65(11), pp.9153-9167.
90. Chen, C., Hu, J., Sui, J. and Zhou, Y., 2017. An information congestion control scheme in the Internet of Vehicles: A bargaining game approach. *Computers & Electrical Engineering*, 58, pp.282-298.
91. Zemouri, S., Djahel, S. and Murphy, J., 2018. An altruistic prediction-based congestion control for strict beaconing requirements in urban VANETs. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 49(12), pp.2582-2597.
92. Li, W., Song, W., Lu, Q. and Yue, C., 2020. Reliable congestion control mechanism for safety applications in urban VANETs. *Ad Hoc Networks*, 98, p.102033.
93. Liu, X. and Jaekel, A., 2019. Congestion control in V2V safety communication: Problem, analysis, approaches. *Electronics*, 8(5), p.540.
94. Jobaer, S., Zhang, Y., Iqbal Hussain, M.A. and Ahmed, F., 2020. UAV-assisted hybrid scheme for urban road safety based on VANETs. *Electronics*, 9(9), p.1499.
95. Cho, B.M., Jang, M.S. and Park, K.J., 2020. Channel-aware congestion control in vehicular cyber-physical systems. *IEEE Access*, 8, pp.73193-73203.
96. Regin, R. and Menakadevi, T., 2019. Dynamic clustering mechanism to avoid congestion control in vehicular ad hoc networks based on node density. *Wireless Personal Communications*, 107(4), pp.1911-1931.
97. Günther, H.J., Riebl, R., Wolf, L. and Facchi, C., 2018. The effect of decentralized congestion control on collective perception in dense traffic scenarios. *Computer Communications*, 122, pp.76-83.
98. Shahi, G.S., Batth, R.S. and Egerton, S., 2020. MRGM: An adaptive mechanism for congestion control in smart vehicular network. *International Journal of Communication Networks and Information Security*, 12(2), pp.273-280.

99. Wang, M., Chen, T., Du, F., Wang, J., Yin, G. and Zhang, Y., 2020. Research on adaptive beacon message transmission power in VANETs. *Journal of Ambient Intelligence and Humanized Computing*, pp.1-13.
100. Sewalkar, P. and Seitz, J., 2020. MC-COCO4V2P: Multi-Channel Clustering-Based Congestion Control for Vehicle-to-Pedestrian Communication. *IEEE Transactions on Intelligent Vehicles*, 6(3), pp.523-532.
101. Goudarzi, F. and Asgari, H., 2017. Non-cooperative beacon rate and awareness control for VANETs. *IEEE Access*, 5, pp.16858-16870.
102. Djahel, S. and Ghamri-Doudane, Y., 2012, April. A robust congestion control scheme for fast and reliable dissemination of safety messages in VANETs. In *2012 IEEE Wireless Communications and Networking Conference (WCNC)* (pp. 2264-2269). IEEE.
103. Sepulcre, M., Gozalvez, J., Härri, J. and Hartenstein, H., 2010. Application-based congestion control policy for the communication channel in VANETs. *IEEE Communications Letters*, 14(10), pp.951-953.
104. Kuhl Morgen, S., Festag, A. and Fettweis, G., 2017, March. Evaluation of multi-hop packet prioritization for decentralized congestion control in vanets. In *2017 IEEE Wireless Communications and Networking Conference (WCNC)* (pp. 1-6). IEEE.
105. Sahoo, J., Wu, E.H.K., Sahu, P.K. and Gerla, M., 2013. Congestion-controlled-coordinator-based MAC for safety-critical message transmission in VANETs. *IEEE transactions on intelligent transportation systems*, 14(3), pp.1423-1437.
106. Bouassida, M.S. and Shawky, M., 2010. A cooperative congestion control approach within VANETs: formal verification and performance evaluation. *EURASIP Journal on Wireless Communications and Networking*, 2010, pp.1-13.
107. Ye, F., Yim, R., Zhang, J. and Roy, S., 2010, May. Congestion control to achieve optimal broadcast efficiency in VANETs. In *2010 IEEE International Conference on Communications* (pp. 1-5). IEEE.

108. Jabbarpour, M.R., Noor, R.M., Khokhar, R.H. and Ke, C.H., 2014. Cross-layer congestion control model for urban vehicular environments. *Journal of Network and Computer Applications*, 44, pp.1-16.
109. Tielert, T., Jiang, D., Chen, Q., Delgrossi, L. and Hartenstein, H., 2011, November. Design methodology and evaluation of rate adaptation based congestion control for vehicle safety communications. In *2011 IEEE vehicular networking conference (VNC)* (pp. 116-123). IEEE.
110. Vesco, A., Scopigno, R., Casetti, C. and Chiasserini, C.F., 2013, December. Investigating the effectiveness of decentralized congestion control in vehicular networks. In *2013 IEEE Globecom Workshops (GC Wkshps)* (pp. 1314-1319). IEEE.
111. Chakroun, O. and Cherkaoui, S., 2014. Overhead-free congestion control and data dissemination for 802.11 p VANETs. *Vehicular Communications*, 1(3), pp.123-133.
112. Aygun, B., Boban, M. and Wyglinski, A.M., 2016. ECPR: Environment-and context-aware combined power and rate distributed congestion control for vehicular communications. *Computer Communications*, 93, pp.3-16.
113. Nafi, N.S., Khan, R.H., Khan, J.Y. and Gregory, M., 2014, November. A predictive road traffic management system based on vehicular ad-hoc network. In *2014 Australasian Telecommunication Networks and Applications Conference (ATNAC)* (pp. 135-140). IEEE.
114. Haouari, N., Moussaoui, S., Senouci, S.M., Boualouache, A. and Messous, M.A., 2017, May. An efficient management of the control channel bandwidth in VANETs. In *2017 IEEE international conference on communications (ICC)* (pp. 1-6). IEEE.
115. Regin, R. and Menakadevi, T., 2021. A novel clustering technique to stop congestion occur vehicular ad-hoc networks using node density based on received signal strength. *Peer-to-Peer Networking and Applications*, 14(4), pp.2361-2371.
116. de Sousa, R.S., Boukerche, A. and Loureiro, A.A., 2020. A distributed and low-overhead traffic congestion control protocol for vehicular ad hoc networks. *Computer Communications*, 159, pp.258-270.

117. Amer, H., Al-Kashoash, H., Khami, M.J., Mayfield, M. and Mihaylova, L., 2020. Non-cooperative game based congestion control for data rate optimization in vehicular ad hoc networks. *Ad Hoc Networks*, 107, p.102181.
118. Fatemidokht, H. and Rafsanjani, M.K., 2020. QMM-VANET: An efficient clustering algorithm based on QoS and monitoring of malicious vehicles in vehicular ad hoc networks. *Journal of Systems and Software*, 165, p.110561.
119. Lakshmanaprabu, S.K., Shankar, K., Rani, S.S., Abdulhay, E., Arunkumar, N., Ramirez, G. and Uthayakumar, J., 2019. An effect of big data technology with ant colony optimization based routing in vehicular ad hoc networks: Towards smart cities. *Journal of cleaner production*, 217, pp.584-593.
120. Zhang, W., Aung, N., Dhelim, S. and Ai, Y., 2018. DIFTOS: A distributed infrastructure-free traffic optimization system based on vehicular ad hoc networks for urban environments. *Sensors*, 18(8), p.2567.
121. Wang, J., Yang, X., Liu, Y. and Qian, Z., 2019. A contention-based hop-by-hop bidirectional congestion control algorithm for ad-hoc networks. *Sensors*, 19(16), p.3484.
122. Sharma, V.K. and Kumar, M., 2017. Adaptive congestion control scheme in mobile ad-hoc networks. *Peer-to-Peer Networking and Applications*, 10(3), pp.633-657.
123. Rajesh, M. and Gnanasekar, J.M., 2016. Congestion control using aodv protocol scheme for wireless ad-hoc network. *Advances in Computer Science and Engineering*, 16(1/2), p.19.
124. Rajesh, M. and Gnanasekar, J.M., 2017. Congestion control scheme for heterogeneous wireless ad hoc networks using self-adjust hybrid model. *International Journal of Pure and Applied Mathematics*, 116(21), pp.519-536.

125. Muchtar, F., Al-Adhaileh, M.H., Alubady, R., Singh, P.K., Ambar, R. and Stiawan, D., 2020. Congestion control for named data networking-based wireless ad hoc network. In *Proceedings of First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019)* (pp. 121-138). Springer, Singapore.
126. Liaqat, H.B., Ali, A., Qadir, J., Bashir, A.K., Bilal, M. and Majeed, F., 2019. Socially-aware congestion control in ad-hoc networks: Current status and the way forward. *Future Generation Computer Systems*, 97, pp.634-660.
127. Kumar, J., Singh, A. and Bhadauria, H.S., 2021. Congestion control load balancing adaptive routing protocols for random waypoint model in mobile ad-hoc networks. *Journal of Ambient Intelligence and Humanized Computing*, 12(5), pp.5479-5487.
128. Srivastava, A., Prakash, A. and Tripathi, R., 2020. Location based routing protocols in VANET: Issues and existing solutions. *Vehicular Communications*, 23, p.100231.
129. Karimi, R. and Shokrollahi, S., 2018. PGRP: Predictive geographic routing protocol for VANETs. *Computer Networks*, 141, pp.67-81.
130. Rana, K.K., Tripathi, S. and Raw, R.S., 2018. Analytical analysis of improved directional location added routing protocol for VANETS. *Wireless Personal Communications*, 98(2), pp.2403-2426.
131. Khan, S., Alam, M., Fränzle, M., Müllner, N. and Chen, Y., 2018. A Traffic Aware Segment-based Routing protocol for VANETs in urban scenarios. *Computers & Electrical Engineering*, 68, pp.447-462.
132. Nebbou, T., Lehsaini, M. and Fouchal, H., 2019. Partial backwards routing protocol for VANETs. *Vehicular Communications*, 18, p.100162.
133. Bagherlou, H. and Ghaffari, A., 2018. A routing protocol for vehicular ad hoc networks using simulated annealing algorithm and neural networks. *The Journal of Supercomputing*, 74(6), pp.2528-2552.

134. Ghaffari, A., 2020. Hybrid opportunistic and position-based routing protocol in vehicular ad hoc networks. *Journal of Ambient Intelligence and Humanized Computing*, 11(4), pp.1593-1603.
135. Ghaffari, A., 2020. Hybrid opportunistic and position-based routing protocol in vehicular ad hoc networks. *Journal of Ambient Intelligence and Humanized Computing*, 11(4), pp.1593-1603.
136. Ramamoorthy, R. and Thangavelu, M., 2021. An enhanced hybrid ant colony optimization routing protocol for vehicular ad-hoc networks. *Journal of Ambient Intelligence and Humanized Computing*, pp.1-32.
137. Joshua, C.J. and Varadarajan, V., 2021. An optimization framework for routing protocols in VANETs: A multi-objective firefly algorithm approach. *Wireless Networks*, 27(8), pp.5567-5576.
138. Poonia, R.C., 2018. A performance evaluation of routing protocols for vehicular ad hoc networks with swarm intelligence. *International Journal of System Assurance Engineering and Management*, 9(4), pp.830-835.
139. Satheshkumar, K. and Mangai, S., 2021. EE-FMDRP: energy efficient-fast message distribution routing protocol for vehicular ad-hoc networks. *Journal of Ambient Intelligence and Humanized Computing*, 12(3), pp.3877-3888.
140. Haider, S., Abbas, G., Abbas, Z.H. and Baker, T., 2019. DABFS: A robust routing protocol for warning messages dissemination in VANETs. *Computer Communications*, 147, pp.21-34.
141. Oche, M., Tambuwal, A.B., Chemebe, C., Noor, R.M. and Distefano, S., 2020. VANETs QoS-based routing protocols based on multi-constrained ability to support ITS infotainment services. *Wireless Networks*, 26(3), pp.1685-1715.
142. Cárdenas, L.L., Mezher, A.M., Bautista, P.A.B. and Igartua, M.A., 2019. A probability-based multimetric routing protocol for vehicular ad hoc networks in urban scenarios. *IEEE access*, 7, pp.178020-178032.

143. Ahamed, A. and Vakilzadian, H., 2018, May. Issues and challenges in VANET routing protocols. In 2018 IEEE international conference on electro/information technology (EIT) (pp. 0723-0728). IEEE.
144. Oubbati, O.S., Chaib, N., Lakas, A., Lorenz, P. and Rachedi, A., 2019. UAV-assisted supporting services connectivity in urban VANETs. *IEEE Transactions on Vehicular Technology*, 68(4), pp.3944-3951.
145. Allani, S., Yeferny, T., Chbeir, R. and Yahia, S.B., 2020. Towards a smarter directional data aggregation in VANETs. *World Wide Web*, 23(4), pp.2303-2322.
146. Oubbati, O.S., Chaib, N., Lakas, A., Lorenz, P. and Rachedi, A., 2019. UAV-assisted supporting services connectivity in urban VANETs. *IEEE Transactions on Vehicular Technology*, 68(4), pp.3944-3951.
147. Allani, S., Yeferny, T., Chbeir, R. and Yahia, S.B., 2020. Towards a smarter directional data aggregation in VANETs. *World Wide Web*, 23(4), pp.2303-2322.
148. Allani, S., Yeferny, T., Chbeir, R. and Yahia, S.B., 2020. Towards a smarter directional data aggregation in VANETs. *World Wide Web*, 23(4), pp.2303-2322.
149. Abuashour, A. and Kadoch, M., 2017. Performance improvement of cluster-based routing protocol in VANET. *Ieee access*, 5, pp.15354-15371.
150. Malik, S. and Sahu, P.K., 2019. A comparative study on routing protocols for VANETs. *Heliyon*, 5(8), p.e02340.
151. Muniyandi, R.C., Qamar, F. and Jasim, A.N., 2020. Genetic optimized location aided routing protocol for VANET based on rectangular estimation of position. *Applied Sciences*, 10(17), p.5759.
152. Raw, R.S., Lobiyal, D.K., Das, S. and Kumar, S., 2015. Analytical evaluation of directional-location aided routing protocol for VANETs. *Wireless Personal Communications*, 82(3), pp.1877-1891.
153. Tian, D., Zheng, K., Zhou, J., Duan, X., Wang, Y., Sheng, Z. and Ni, Q., 2017. A microbial inspired routing protocol for VANETs. *IEEE Internet of Things Journal*, 5(4), pp.2293-2303.

154. Abbasi, I.A., Khan, A.S. and Ali, S., 2018. Dynamic multiple junction selection based routing protocol for VANETs in city environment. *Applied Sciences*, 8(5), p.687.
155. Shrivastava, P.K. and Vishwamitra, L.K., 2021. Comparative analysis of proactive and reactive routing protocols in VANET environment. *Measurement: Sensors*, 16, p.100051.
156. García-Campos, J.M., Sánchez-García, J., Reina, D.G., Toral, S.L. and Barrero, F., 2016. An evaluation methodology for reliable simulation based studies of routing protocols in VANETs. *Simulation modelling practice and theory*, 66, pp.139-165.
157. Oubbati, O.S., Lakas, A., Zhou, F., Güneş, M., Lagraa, N. and Yagoubi, M.B., 2017. Intelligent UAV-assisted routing protocol for urban VANETs. *Computer communications*, 107, pp.93-111.
158. Moridi, E. and Barati, H., 2017. RMRPTS: a reliable multi-level routing protocol with tabu search in VANET. *Telecommunication Systems*, 65(1), pp.127-137.
159. Mohaisen, L.F. and Joiner, L.L., 2017. Interference aware bandwidth estimation for load balancing in EMHR-energy based with mobility concerns hybrid routing protocol for VANET-WSN communication. *Ad Hoc Networks*, 66, pp.1-15.
160. Aravindhana, K. and Dhas, C., 2019. Destination-aware context-based routing protocol with hybrid soft computing cluster algorithm for VANET. *Soft Computing*, 23(8), pp.2499-2507.
161. Bangui, H., Ge, M. and Buhnova, B., 2022. A hybrid machine learning model for intrusion detection in vanet. *Computing*, 104(3), pp.503-531.
162. Nadarajan, J. and Kaliyaperumal, J., 2021. QOS aware and secured routing algorithm using machine intelligence in next generation VANET. *International Journal of System Assurance Engineering and Management*, pp.1-12.
163. Wu, J., Fang, M., Li, H. and Li, X., 2020. RSU-assisted traffic-aware routing based on reinforcement learning for urban vanets. *IEEE Access*, 8, pp.5733-5748.

164. Tang, Y., Cheng, N., Wu, W., Wang, M., Dai, Y. and Shen, X., 2019. Delay-minimization routing for heterogeneous VANETs with machine learning based mobility prediction. *IEEE Transactions on Vehicular Technology*, 68(4), pp.3967-3979.
165. Ji, X., Xu, W., Zhang, C., Yun, T., Zhang, G., Wang, X., Wang, Y. and Liu, B., 2019, July. Keep forwarding path freshest in VANET via applying reinforcement learning. In *2019 IEEE First International Workshop on Network Meets Intelligent Computations (NMIC)* (pp. 13-18). IEEE.
166. Zhang, D., Zhang, T. and Liu, X., 2019. Novel self-adaptive routing service algorithm for application in VANET. *Applied Intelligence*, 49(5), pp.1866-1879.
Zhang, D., Zhang, T. and Liu, X., 2019. Novel self-adaptive routing service algorithm for application in VANET. *Applied Intelligence*, 49(5), pp.1866-1879.
167. Guo, X., Chen, Y., Cao, L., Zhang, D. and Jiang, Y., 2020. A receiver-forwarding decision scheme based on Bayesian for NDN-VANET. *China Communications*, 17(8), pp.106-120.
168. Li, F., Song, X., Chen, H., Li, X. and Wang, Y., 2018. Hierarchical routing for vehicular ad hoc networks via reinforcement learning. *IEEE Transactions on Vehicular Technology*, 68(2), pp.1852-1865.
169. Sharshembiev, K., Yoo, S.M. and Elmahdi, E., 2021. Protocol misbehavior detection framework using machine learning classification in vehicular Ad Hoc networks. *Wireless Networks*, 27(3), pp.2103-2118.
170. Yu, K., Tan, L.Z., Wu, X.J. and Gai, Z.Y., 2019, November. Machine learning driven network routing. In *2019 6th International Conference on Systems and Informatics (ICSAI)* (pp. 705-712). IEEE.
171. Gupta, N., Jain, A., Vaisla, K.S., Kumar, A. and Kumar, R., 2021. Performance analysis of DSDV and OLSR wireless sensor network routing protocols using FPGA hardware and machine learning. *Multimedia Tools and Applications*, 80(14), pp.22301-22319.

172. Sharshembiev, K., Yoo, S.M. and Elmahdi, E., 2021. Protocol misbehavior detection framework using machine learning classification in vehicular Ad Hoc networks. *Wireless Networks*, 27(3), pp.2103-2118.
173. Yu, K., Tan, L.Z., Wu, X.J. and Gai, Z.Y., 2019, November. Machine learning driven network routing. In *2019 6th International Conference on Systems and Informatics (ICSAI)* (pp. 705-712). IEEE.
174. Gupta, N., Jain, A., Vaisla, K.S., Kumar, A. and Kumar, R., 2021. Performance analysis of DSDV and OLSR wireless sensor network routing protocols using FPGA hardware and machine learning. *Multimedia Tools and Applications*, 80(14), pp.22301-22319.
175. Grover, J., Prajapati, N.K., Laxmi, V. and Gaur, M.S., 2011, July. Machine learning approach for multiple misbehavior detection in VANET. In *International conference on advances in computing and communications* (pp. 644-653). Springer, Berlin, Heidelberg.
176. Wu, C., Yoshinaga, T., Ji, Y., Murase, T. and Zhang, Y., 2016. A reinforcement learning-based data storage scheme for vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, 66(7), pp.6336-6348.
177. Soua, A. and Afifi, H., 2013, July. Adaptive data collection protocol using reinforcement learning for VANETs. In *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)* (pp. 1040-1045). IEEE.
178. Wu, C., Ohzahata, S. and Kato, T., 2013. Flexible, portable, and practicable solution for routing in VANETs: A fuzzy constraint Q-learning approach. *IEEE Transactions on Vehicular Technology*, 62(9), pp.4251-4263.
179. Wu, C., Chen, X., Ji, Y., Liu, F., Ohzahata, S., Yoshinaga, T. and Kato, T., 2015. Packet size-aware broadcasting in VANETs with fuzzy logic and RL-based parameter adaptation. *IEEE Access*, 3, pp.2481-2491.

180. Shilova, Y., Kavalero, M. and Bezukladnikov, I., 2016, February. Full Echo Q-routing with adaptive learning rates: a reinforcement learning approach to network routing. In *2016 IEEE NW Russia Young Researchers in Electrical and Electronic Engineering Conference (EIconRusNW)* (pp. 341-344). IEEE.
181. Mohammadnezhad, M. and Ghaffari, A., 2019. Hybrid routing scheme using imperialist competitive algorithm and RBF neural networks for VANETs. *Wireless Networks*, 25(5), pp.2831-2849.
182. Nahar, A. and Das, D., 2020, June. Adaptive reinforcement routing in software defined vehicular networks. In *2020 International Wireless Communications and Mobile Computing (IWCMC)* (pp. 2118-2123). IEEE.
183. 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.
184. Zhang, H., Bochem, A., Sun, X. and Hogrefe, D., 2018, June. A security aware fuzzy enhanced reliable ant colony optimization routing in vehicular ad hoc networks. In *2018 IEEE Intelligent Vehicles Symposium (IV)* (pp. 1071-1078). IEEE.
185. Thilak, K.D. and Amuthan, A.J.F.G.C.S., 2018. Cellular automata-based improved ant colony-based optimization algorithm for mitigating ddos attacks in vanets. *Future Generation Computer Systems*, 82, pp.304-314.
186. Thilak, K.D. and Amuthan, A.J.F.G.C.S., 2018. Cellular automata-based improved ant colony-based optimization algorithm for mitigating ddos attacks in vanets. *Future Generation Computer Systems*, 82, pp.304-314.
187. Prabakeran, S. and Sethukarasi, T., 2020. Optimal solution for malicious node detection and prevention using hybrid chaotic particle dragonfly swarm algorithm in VANETs. *Wireless Networks*, 26(8), pp.5897-5917.
188. Fatemidokht, H., Rafsanjani, M.K., Gupta, B.B. and Hsu, C.H., 2021. Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular ad hoc networks in intelligent transportation systems. *IEEE Transactions on Intelligent Transportation Systems*, 22(7), pp.4757-4769.

189. Khare, N., Devan, P., Chowdhary, C.L., Bhattacharya, S., Singh, G., Singh, S. and Yoon, B., 2020. SMO-DNN: spider monkey optimization and deep neural network hybrid classifier model for intrusion detection. *Electronics*, 9(4), p.692.
190. Krundyshev, V., Kalinin, M. and Zegzhda, P., 2018, May. Artificial swarm algorithm for VANET protection against routing attacks. In *2018 IEEE Industrial Cyber-Physical Systems (ICPS)* (pp. 795-800). IEEE.
191. Kerrache, C.A., Lakas, A., Lagraa, N. and Barka, E., 2018. UAV-assisted technique for the detection of malicious and selfish nodes in VANETs. *Vehicular Communications*, 11, pp.1-11.
192. Balamurugan, A., Priya, M., Malar, A. and Janakiraman, S., 2021. Raccoon optimization algorithm-based accurate positioning scheme for reliable emergency data dissemination under NLOS situations in VANETs. *Journal of Ambient Intelligence and Humanized Computing*, 12(11), pp.10405-10424.
193. Kerrache, C.A., Lakas, A., Lagraa, N. and Barka, E., 2018. UAV-assisted technique for the detection of malicious and selfish nodes in VANETs. *Vehicular Communications*, 11, pp.1-11.
194. Tripathi, K.N., Jain, G., Yadav, A.M. and Sharma, S.C., 2021. Entity-centric combined trust (ECT) algorithm to detect packet dropping attack in vehicular Ad Hoc Networks (VANETs). In *Next Generation Information Processing System* (pp. 23-33). Springer, Singapore.
195. Balamurugan, A., Priya, M., Malar, A. and Janakiraman, S., 2021. Raccoon optimization algorithm-based accurate positioning scheme for reliable emergency data dissemination under NLOS situations in VANETs. *Journal of Ambient Intelligence and Humanized Computing*, 12(11), pp.10405-10424.
196. Khare, N., Devan, P., Chowdhary, C.L., Bhattacharya, S., Singh, G., Singh, S. and Yoon, B., 2020. SMO-DNN: spider monkey optimization and deep neural network hybrid classifier model for intrusion detection. *Electronics*, 9(4), p.692.

197. Awan, K.A., Din, I.U., Almogren, A., Guizani, M. and Khan, S., 2020. StabTrust—A stable and centralized trust-based clustering mechanism for IoT enabled vehicular ad-hoc networks. *Ieee Access*, 8, pp.21159-21177.
198. Wahab, O.A., Mourad, A., Otrouk, H. and Bentahar, J., 2016. CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks. *Expert Systems with Applications*, 50, pp.40-54.
199. 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.
200. Tolba, A.M.R., 2018. Trust-based distributed authentication method for collision attack avoidance in VANETs. *IEEE Access*, 6, pp.62747-62755.
201. Mirsadeghi, F., Rafsanjani, M.K. and Gupta, B.B., 2021. A trust infrastructure based authentication method for clustered vehicular ad hoc networks. *Peer-to-Peer Networking and Applications*, 14(4), pp.2537-2553.
202. Zhang, C., Chen, K., Zeng, X. and Xue, X., 2018. Misbehavior detection based on support vector machine and Dempster-Shafer theory of evidence in VANETs. *IEEE Access*, 6, pp.59860-59870.
203. Velayudhan, N.C., Anitha, A. and Madanan, M., 2021. Sybil Attack with RSU Detection and Location Privacy in Urban VANETs: An Efficient EPORP Technique. *Wireless Personal Communications*, pp.1-29.
204. Malik, N., Nanda, P., He, X. and Liu, R.P., 2020. Vehicular networks with security and trust management solutions: proposed secured message exchange via blockchain technology. *Wireless Networks*, 26(6), pp.4207-4226.
205. A Ghaleb, F., Saeed, F., Al-Sarem, M., Ali Saleh Al-rimy, B., Boulila, W., Eljaily, 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.

206. 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.
207. Shams, E.A., Rizaner, A. and Ulusoy, A.H., 2018. Trust aware support vector machine intrusion detection and prevention system in vehicular ad hoc networks. *Computers & Security*, 78, pp.245-254.
208. Poongodi, M., Vijayakumar, V., Al-Turjman, F., Hamdi, M. and Ma, M., 2019. Intrusion prevention system for DDoS attack on VANET with reCAPTCHA controller using information based metrics. *IEEE Access*, 7, pp.158481-158491.
209. Dey, S., Ye, Q. and Sampalli, S., 2019. A machine learning based intrusion detection scheme for data fusion in mobile clouds involving heterogeneous client networks. *Information Fusion*, 49, pp.205-215.
210. Khot, P.S. and Naik, U., 2021. Particle-Water Wave Optimization for Secure Routing in Wireless Sensor Network Using Cluster Head Selection. *Wireless Personal Communications*, 119(3), pp.2405-2429.
211. Eiza, M.H., Owens, T. and Ni, Q., 2015. Secure and robust multi-constrained QoS aware routing algorithm for VANETs. *IEEE Transactions on Dependable and Secure Computing*, 13(1), pp.32-45.
212. Moadeli, M. and Vanderbauwhede, W., 2011. An analytical model of broadcast in QoS-aware wormhole-routed NoCs. *Journal of Systems and Software*, 84(1), pp.12-20.
213. Demir, K., Germanus, D. and Suri, N., 2017. Robust QoS-aware communication in the smart distribution grid. *Peer-to-Peer Networking and Applications*, 10(1), pp.193-207.
214. Tao, J., Zhu, L., Wang, X., He, J. and Liu, Y., 2014, December. RSU deployment scheme with power control for highway message propagation in VANETs. In *2014 IEEE Global Communications Conference* (pp. 169-174). IEEE.

215. Makmal, A., Melnikov, A.A., Dunjko, V. and Briegel, H.J., 2016. Meta-learning within projective simulation. *IEEE Access*, 4, pp.2110-2122.
216. Mchergui, A., Moulahi, T. and Nasri, S., 2020. BaaS: Broadcast as a service cross-layer learning-based approach in cloud assisted VANETs. *Computer networks*, 182, p.107468.
217. Ramamoorthi, J.S. and Sangaiah, A.K., 2019. SCGR: Self-configuring greedy routing for minimizing routing interrupts in vehicular communication networks. *Internet of Things*, 8, p.100108.
218. Ramamoorthi, J.S. and Sangaiah, A.K., 2019. SCGR: Self-configuring greedy routing for minimizing routing interrupts in vehicular communication networks. *Internet of Things*, 8, p.100108.
219. Lu, C., Wang, Z., Ding, W., Li, G., Liu, S. and Cheng, L., 2021. MARVEL: Multi-agent reinforcement learning for VANET delay minimization. *China Communications*, 18(6), pp.1-11.
220. Luo, L., Sheng, L., Yu, H. and Sun, G., 2021. Intersection-Based V2X Routing via Reinforcement Learning in Vehicular Ad Hoc Networks. *IEEE Transactions on Intelligent Transportation Systems*.
221. Celes, C., Boukerche, A. and Loureiro, A.A., 2020. From mobility traces to knowledge: Design guidance for intelligent vehicular networks. *IEEE Network*, 34(4), pp.227-233.
222. Alghamdi, S.A., 2021. Cellular V2X With D2D Communications for Emergency Message Dissemination and QoS Assured Routing in 5G Environment. *IEEE Access*, 9, pp.56049-56065.
223. Al-Rabayah, M. and Malaney, R., 2012. A new scalable hybrid routing protocol for VANETs. *IEEE transactions on vehicular technology*, 61(6), pp.2625-2635.
224. Bitam, S., Mellouk, A. and Zeadally, S., 2013. HyBR: A hybrid bio-inspired bee swarm routing protocol for safety applications in vehicular ad hoc networks (VANETs). *Journal of Systems Architecture*, 59(10), pp.953-967.

225. Ayaida, M., Barhoumi, M., Fouchal, H., Ghamri-Doudane, Y. and Afilal, L., 2013, June. Phrhls: A movement-prediction-based joint routing and hierarchical location service for vanets. In *2013 IEEE international conference on communications (ICC)* (pp. 1424-1428). IEEE.
226. Wu, D., Zhang, Y., Bao, L. and Regan, A.C., 2013. Location-based crowdsourcing for vehicular communication in hybrid networks. *IEEE transactions on intelligent transportation systems*, 14(2), pp.837-846.
227. Safavat, S. and Rawat, D.B., 2020. On the elliptic curve cryptography for privacy-aware secure ACO-AODV routing in intent-based internet of vehicles for smart cities. *IEEE Transactions on Intelligent Transportation Systems*, 22(8), pp.5050-5059.
228. Rovira-Sugranes, A., Razi, A., Afghah, F. and Chakareski, J., 2022. A review of AI-enabled routing protocols for UAV networks: Trends, challenges, and future outlook. *Ad Hoc Networks*, p.102790.
229. Bousbaa, F.Z., Kerrache, C.A., Mahi, Z., Tahari, A.E.K., Lagraa, N. and Yagoubi, M.B., 2020. GeoUAVs: A new geocast routing protocol for fleet of UAVs. *Computer Communications*, 149, pp.259-269.
230. Gomathi, N. and Wagh, M.B., 2021. Improved rider for vehicular adhocNETwork routing via neural network. *Evolutionary Intelligence*, pp.1-14.
231. Samriya, J.K. and Kumar, N., 2020. A novel intrusion detection system using hybrid clustering-optimization approach in cloud computing. *Materials Today: Proceedings*.
232. Bu, S.J., Kang, H.B. and Cho, S.B., 2022. Ensemble of Deep Convolutional Learning Classifier System Based on Genetic Algorithm for Database Intrusion Detection. *Electronics*, 11(5), p.745.
233. Priya, J.S., Bhaskar, N. and Prabakeran, S., 2021. Fuzzy with black widow and spider monkey optimization for privacy-preserving-based crowdsourcing system. *Soft Computing*, 25(7), pp.5831-5846.

234. Alex, S. and Rajkumar, T.D., 2021. Spider bird swarm algorithm with deep belief network for malicious JavaScript detection. *Computers & Security*, 107, p.102301.
235. Kalinin, M.O., Zubkov, E.A., Suprun, A.F. and Pechenkin, A.I., 2018. Prevention of attacks on dynamic routing in self-organizing adhoc networks using swarm intelligence. *Automatic Control and Computer Sciences*, 52(8), pp.977-983.
236. Kumar, A. and Gupta, N., 2020, December. A Secure RSU based Security against Multiple Attacks in VANET. In *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)* (pp. 1156-1163). IEEE.
237. Erskine, S.K. and Elleithy, K.M., 2019. Real-time detection of DoS attacks in IEEE 802.11 p using fog computing for a secure intelligent vehicular network. *Electronics*, 8(7), p.776.
238. Zhang, Z., Long, K., Wang, J. and Dressler, F., 2013. On swarm intelligence inspired self-organized networking: its bionic mechanisms, designing principles and optimization approaches. *IEEE Communications Surveys & Tutorials*, 16(1), pp.513-537.
239. Lee, S.W., Mohammadi, M., Rashidi, S., Rahmani, A.M., Masdari, M. and Hosseinzadeh, M., 2021. Towards secure intrusion detection systems using deep learning techniques: Comprehensive analysis and review. *Journal of Network and Computer Applications*, 187, p.103111.
240. Asghar, M.Z., Abbas, M., Zeeshan, K., Kotilainen, P. and Hämäläinen, T., 2019. Assessment of deep learning methodology for self-organizing 5g networks. *Applied Sciences*, 9(15), p.2975.
241. Haddadou, N., Rachedi, A. and Ghamri-Doudane, Y., 2014. A job market signaling scheme for incentive and trust management in vehicular ad hoc networks. *IEEE transactions on vehicular technology*, 64(8), pp.3657-3674.
242. Alheeti, K.M.A., Gruebler, A. and McDonald-Maier, K., 2017. Using discriminant analysis to detect intrusions in external communication for self-driving vehicles. *Digital Communications and Networks*, 3(3), pp.180-187.

243. Tripathi, K.N. and Sharma, S.C., 2020. A trust based model (TBM) to detect rogue nodes in vehicular ad-hoc networks (VANETS). *International Journal of System Assurance Engineering and Management*, 11(2), pp.426-440.
244. Oubabas, S., Aoudjit, R., Rodrigues, J.J. and Talbi, S., 2018. Secure and stable vehicular ad hoc network clustering algorithm based on hybrid mobility similarities and trust management scheme. *Vehicular Communications*, 13, pp.128-138.
245. Divya, N.S., Bobba, V. and Vatambeti, R., 2021. An adaptive cluster based vehicular routing protocol for secure communication. *Wireless Personal Communications*, pp.1-20.
246. Yao, X., Zhang, X., Ning, H. and Li, P., 2017. Using trust model to ensure reliable data acquisition in VANETs. *Ad Hoc Networks*, 55, pp.107-118.
247. Ahmad, F., Kurugollu, F., Adnane, A., Hussain, R. and Hussain, F., 2020. MARINE: Man-in-the-middle attack resistant trust model in connected vehicles. *IEEE Internet of Things Journal*, 7(4), pp.3310-3322.
248. Shaaban, R., 2021. *Visible Light Communication Cyber Security Vulnerabilities For Indoor And Outdoor Vehicle-To-Vehicle Communication* (Doctoral dissertation, The University of North Dakota).
249. Abdel Hakeem, S.A., Hussein, H.H. and Kim, H., 2022. Security Requirements and Challenges of 6G Technologies and Applications. *Sensors*, 22(5), p.1969.
250. Chembe, C., Noor, R.M., Ahmedy, I., Oche, M., Kunda, D. and Liu, C.H., 2017. Spectrum sensing in cognitive vehicular network: State-of-Art, challenges and open issues. *Computer Communications*, 97, pp.15-30.
251. Awan, K.A., Din, I.U., Almogren, A., Guizani, M. and Khan, S., 2020. StabTrust—A stable and centralized trust-based clustering mechanism for IoT enabled vehicular ad-hoc networks. *Ieee Access*, 8, pp.21159-21177.
252. Haseeb, K., Din, I.U., Almogren, A., Islam, N. and Altameem, A., 2020. RTS: A robust and trusted scheme for IoT-based mobile wireless mesh networks. *IEEE Access*, 8, pp.68379-68390.

253. Awan, K.A., Din, I.U., Almogren, A., Guizani, M., Altameem, A. and Jadoon, S.U., 2019. Robusttrust—a pro-privacy robust distributed trust management mechanism for internet of things. *IEEE Access*, 7, pp.62095-62106.
254. Haseeb, K., Islam, N., Almogren, A. and Din, I.U., 2019. Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things. *Ieee Access*, 7, pp.185496-185505.
255. Jindal, V. and Bedi, P., 2018. An improved hybrid ant particle optimization (IHAPSO) algorithm for reducing travel time in VANETs. *Applied Soft Computing*, 64, pp.526-535.
256. Shukla, R.S., Tyagi, N., Gupta, A. and Dubey, K.K., 2020. A new position based routing algorithm for vehicular ad hoc networks. *Telecommunication Systems*, 75(2), pp.205-220.
257. Jindal, V. and Bedi, P., 2017. Reducing waiting time with parallel preemptive algorithm in VANETs. *Vehicular Communications*, 7, pp.58-65.
258. Singh, R., Saluja, D. and Kumar, S., 2021. Graphical approach for V2V connectivity enhancement in clustering-based VANET. *IEEE Wireless Communications Letters*, 10(6), pp.1217-1221.
259. Al Mallah, R., Quintero, A. and Farooq, B., 2017. Distributed classification of urban congestion using VANET. *IEEE Transactions on Intelligent Transportation Systems*, 18(9), pp.2435-2442.
260. Ullah, A., Yaqoob, S., Imran, M. and Ning, H., 2018. Emergency message dissemination schemes based on congestion avoidance in VANET and vehicular FoG computing. *IEEE Access*, 7, pp.1570-1585.
261. Kumar, R. and Dave, M., 2013. A framework for handling local broadcast storm using probabilistic data aggregation in VANET. *Wireless personal communications*, 72(1), pp.315-341.
262. Giripunje, L.M., Vidyarthi, A. and Shandilya, S.K., 2022. Adaptive Congestion Prediction in Vehicular Ad-hoc Networks (VANET) using Type-2 Fuzzy Model to Establish Reliable Routes. *Wireless Personal Communications*, pp.1-22.

263. Regin, R. and Menakadevi, T., 2021. A novel clustering technique to stop congestion occur vehicular ad-hoc networks using node density based on received signal strength. *Peer-to-Peer Networking and Applications*, 14(4), pp.2361-2371.
264. Sangaiah, A.K., Ramamoorthi, J.S., Rodrigues, J.J., Rahman, M.A., Muhammad, G. and Alrashoud, M., 2020. LACCVoV: linear adaptive congestion control with optimization of data dissemination model in vehicle-to-vehicle communication. *IEEE Transactions on Intelligent Transportation Systems*, 22(8), pp.5319-5328.
265. Ebadinezhad, S., 2021. Design and performance evaluation of Improved DFACO protocol based on dynamic clustering in VANETs. *SN Applied Sciences*, 3(4), pp.1-15.
266. Mohaisen, L.F. and Joiner, L.L., 2017. Interference aware bandwidth estimation for load balancing in EMHR-energy based with mobility concerns hybrid routing protocol for VANET-WSN communication. *Ad Hoc Networks*, 66, pp.1-15.
267. Terroso-Saenz, F., Valdes-Vela, M., Sotomayor-Martinez, C., Toledo-Moreo, R. and Gomez-Skarmeta, A.F., 2012. A cooperative approach to traffic congestion detection with complex event processing and VANET. *IEEE Transactions on Intelligent Transportation Systems*, 13(2), pp.914-929.
268. Yang, A., Weng, J., Cheng, N., Ni, J., Lin, X. and Shen, X., 2019. DeQoS attack: Degrading quality of service in VANETs and its mitigation. *IEEE Transactions on Vehicular Technology*, 68(5), pp.4834-4845.
269. Feukeu, E.A. and Zuva, T., 2020. Dynamic broadcast storm mitigation approach for VANETs. *Future Generation Computer Systems*, 107, pp.1097-1104.
270. Mohammadnezhad, M. and Ghaffari, A., 2019. Hybrid routing scheme using imperialist competitive algorithm and RBF neural networks for VANETs. *Wireless Networks*, 25(5), pp.2831-2849.

271. Bello-Salau, H., Onumanyi, A.J., Abu-Mahfouz, A.M., Adejo, A.O. and Mu'Azu, M.B., 2020. New discrete cuckoo search optimization algorithms for effective route discovery in IoT-based vehicular ad-hoc networks. *IEEE Access*, 8, pp.145469-145488.
272. Kandali, K., Bennis, L. and Bennis, H., 2021. A new hybrid routing protocol using a modified K-means clustering algorithm and continuous hopfield network for VANET. *IEEE Access*, 9, pp.47169-47183.
273. Tang, Y., Cheng, N., Wu, W., Wang, M., Dai, Y. and Shen, X., 2019. Delay-minimization routing for heterogeneous VANETs with machine learning based mobility prediction. *IEEE Transactions on Vehicular Technology*, 68(4), pp.3967-3979.
274. Gnanasekar, T.S. and Samiappan, D., 2021. Impact of hybridized rider optimization with cuckoo search algorithm on optimal VANET routing. *International Journal of Communication Systems*, 34(16), p.e4954.
275. Ramamoorthy, R. and Thangavelu, M., 2021. An enhanced hybrid ant colony optimization routing protocol for vehicular ad-hoc networks. *Journal of Ambient Intelligence and Humanized Computing*, pp.1-32.
276. Outay, F., Mengash, H.A. and Adnan, M., 2020. Applications of unmanned aerial vehicle (UAV) in road safety, traffic and highway infrastructure management: Recent advances and challenges. *Transportation research part A: policy and practice*, 141, pp.116-129.
277. Semiari, O., Saad, W., Bennis, M. and Debbah, M., 2019. Integrated millimeter wave and sub-6 GHz wireless networks: A roadmap for joint mobile broadband and ultra-reliable low-latency communications. *IEEE Wireless Communications*, 26(2), pp.109-115.
278. Fakhfakh, F., Tounsi, M. and Mosbah, M., 2019, June. A comprehensive survey on broadcasting emergency messages. In *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)* (pp. 1983-1988). IEEE.

279. Bilal, R. and Khan, B.M., 2021. The role of vehicular ad hoc networks in intelligent transport systems for healthcare. In *Advances in Multidisciplinary Medical Technologies— Engineering, Modeling and Findings* (pp. 155-183). Springer, Cham.
280. Shrivastava, P.K. and Vishwamitra, L.K., 2021. Comparative analysis of proactive and reactive routing protocols in VANET environment. *Measurement: Sensors*, 16, p.100051.
281. Huang, Y., Ding, H., Zhang, Y., Wang, H., Cao, D., Xu, N. and Hu, C., 2019. A motion planning and tracking framework for autonomous vehicles based on artificial potential field elaborated resistance network approach. *IEEE Transactions on Industrial Electronics*, 67(2), pp.1376-1386.
282. Ghaffari, A., 2020. Hybrid opportunistic and position-based routing protocol in vehicular ad hoc networks. *Journal of Ambient Intelligence and Humanized Computing*, 11(4), pp.1593-1603.
283. Malhi, A.K., Batra, S. and Pannu, H.S., 2020. Security of vehicular ad-hoc networks: A comprehensive survey. *Computers & Security*, 89, p.101664.
284. Ullah, S., Abbas, G., Abbas, Z.H., Waqas, M. and Ahmed, M., 2020. RBO-EM: Reduced broadcast overhead scheme for emergency message dissemination in VANETs. *IEEE Access*, 8, pp.175205-175219.
285. Brandão, A.S., Lima, M.C., Abbas, C.J.B. and Villalba, L.J.G., 2020. An energy balanced flooding algorithm for a BLE mesh network. *IEEE Access*, 8, pp.97946-97958.
286. Khamer, L., Labraoui, N., Gueroui, A.M., Zaidi, S. and Ari, A.A.A., 2021. Road network layout based multi-hop broadcast protocols for Urban Vehicular Ad-hoc Networks. *Wireless Networks*, 27(2), pp.1369-1388.
287. Abbasi, H.I., Voicu, R.C., Copeland, J.A. and Chang, Y., 2019. Towards fast and reliable multihop routing in VANETs. *IEEE Transactions on Mobile Computing*, 19(10), pp.2461-2474.

288. Saleh, H.H. and Hasson, S.T., 2019, April. A survey of routing algorithms in vehicular networks. In *2019 International Conference on Advanced Science and Engineering (ICOASE)* (pp. 159-164). IEEE.
289. Stanica, R., Chaput, E. and Beylot, A.L., 2012, June. Congestion control in CSMA-based vehicular networks: Do not forget the carrier sensing. In *2012 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)* (pp. 650-658). IEEE.
290. Ryu, M. and Cha, S.H., 2020. Mobility Prediction Based Multi-Directional Broadcasting for Both Highway and Urban Vehicular Sensor Networks. *IEEE Access*, 8, pp.148595-148605.
291. Nadarajan, J. and Kaliyaperumal, J., 2021. QOS aware and secured routing algorithm using machine intelligence in next generation VANET. *International Journal of System Assurance Engineering and Management*, pp.1-12.
292. Boukerche, A. and Wang, J., 2020. A performance modeling and analysis of a novel vehicular traffic flow prediction system using a hybrid machine learning-based model. *Ad Hoc Networks*, 106, p.102224.
293. Hossain, M.A., Md Noor, R., Yau, K.L.A., Azzuhri, S.R., Z'aba, M.R., Ahmedy, I. and Jabbarpour, M.R., 2021. Machine learning-based cooperative spectrum sensing in dynamic segmentation enabled cognitive radio vehicular network. *Energies*, 14(4), p.1169.
294. Tang, F., Kawamoto, Y., Kato, N. and Liu, J., 2019. Future intelligent and secure vehicular network toward 6G: Machine-learning approaches. *Proceedings of the IEEE*, 108(2), pp.292-307.
295. Najm, I.A., Hamoud, A.K., Lloret, J. and Bosch, I., 2019. Machine learning prediction approach to enhance congestion control in 5G IoT environment. *Electronics*, 8(6), p.607.

296. Kaushik, S., Tripathi, K., Gupta, R. and Mahajan, P., 2021, July. Futuristic Analysis of Machine Learning Based Routing Protocols in Wireless Ad Hoc Networks. In *2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT)* (pp. 324-329). IEEE.
297. Ye, M., Guan, L. and Quddus, M., 2019, April. Mpbrp-mobility prediction based routing protocol in vanets. In *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)* (pp. 1-7). IEEE.
298. Abdel-Halim, I.T., Fahmy, H.M.A. and Bahaa-El Din, A.M., 2019. Mobility prediction-based efficient clustering scheme for connected and automated vehicles in VANETs. *Computer Networks*, 150, pp.217-233.
299. Rehman, O., Qureshi, R., Ould-Khaoua, M. and Niazi, M.F., 2020. Analysis of mobility speed impact on end-to-end communication performance in VANETs. *Vehicular Communications*, 26, p.100278.
300. Abdellah, A.R., Muthanna, A. and Koucheryavy, A., 2019. Robust estimation of VANET performance-based robust neural networks learning. In *Internet of Things, smart spaces, and next generation networks and systems* (pp. 402-414). Springer, Cham.
301. Hossain, Mohammad Asif & Md. Noor, Rafidah & Yau, Kok-Lim & Razalli, Saaidal & Zaba, Muhammad & Ahmedy, Ismail & Jabbarpour, Reza. ,2021. Multi-Objective Harris Hawks Optimization Algorithm based 2-hop Routing Algorithm for CR-VANET. *IEEE Access*. 9. 58230 - 58242. 10.1109/ACCESS.2021.3072922.