Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019)
Vol.01/ No. 02
Pages: 76-86
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2019.2.002

EFFICIENT ROUTING PROTOCOL WITH COLLISION AVOIDANCE IN VEHICULAR NETWORKS

Dr. D. Sivaganesan,
Professor, Department of Computer Engineering,
PSG Institute of Technology and Applied Research,
Coimbatore, India.
Email: sivaganesan@psgitech.ac.in

Abstract: The vehicle-Adhoc Networks are the specific type wireless adhoc networks, framed using the group of vehicles supporting the “on the fly’ communication between vehicles on the roadside. This is basically developed to handle the traffic in an intelligent manner avoiding the unnecessary time elapse, discomfort and the fatalities during the travelling and in turn improvise the convenience in the transportation providing a continuous traffic movement. But certain emergent situations such as the natural disasters, accidents, damaged roads, sudden break down of the vehicles and the appearance of the emergency vehicles disturb the regular traffic flow and safety of the on road vehicles. To ensure the safety of on road vehicles and elude the collision of the vehicles that take place due to improper communications or communication attacks, the paper puts forth an effective routing protocol with collision avoidance, (ERPCA) to identify vehicles with the reliability to transfer information on time and evade the discomforts in travelling. The evaluation of the ERPCA with the network simulator-2 evinces the improvement in the performance of the vehicular-adhoc networks.

Keyword: Wireless Adhoc Network, Vehicular-Adhoc Network, Collision Avoidance, ERPCA, and Hybrid Routing

1. INTRODUCTION

Developing a smart city involves the improvements under many areas such as the development of smart homes, smart hospital, smart water system, electricity distribution etc. and smart transportation also takes an important role in turning the cities smart. The intelligent transportation system that remains as the back bone of the smart transportation is founded on the vehicular-adhoc networks [1-5]. The vehicular-adhoc network is a specific type of the wireless-adhoc network that enables the on road vehicles to communicate. This type of network, framed using the supporting vehicles is distributed in nature and has dynamic topologies. The vehicular-adhoc [6] mainly aims in supporting different type of applications such as warnings of traffic conditions, and information’s such as parking availability, shortest route to destination, nearby stay available etc. [7-8].

The vehicular-network communicates in two ways either using the vehicle to vehicle communication and vehicle to road side unit communication [9]. The on board unit installed in the vehicles allows the vehicles to extend communication between vehicles and the road side units. The figure.1 below shows the vehicle to vehicle and the vehicle to infrastructure communication of the vehicular-adhoc network [10][11].

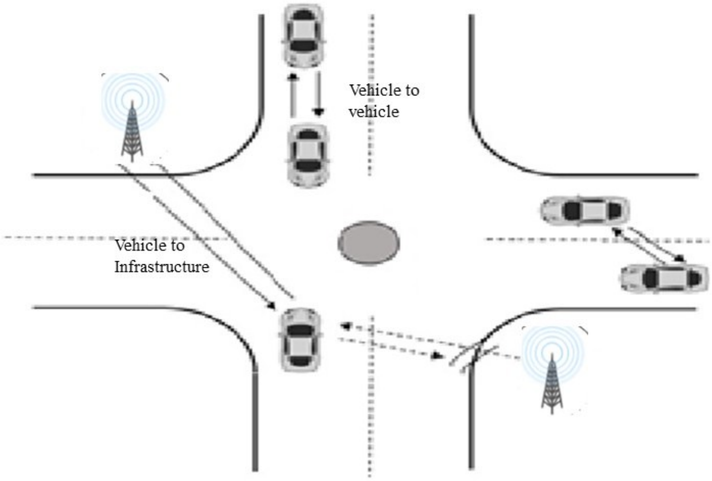


Fig.1 Vehicular Adhoc Network [1]

The vehicle either transmits or receives information using the vehicles or the road side units whichever is close by, the process of vehicle communication enables the vehicular-adhoc to experience various attributes such as the prediction concept, high mobility, geographical communication, changing frequencies and dynamic topologies. Due to its changing topologies and the high mobility routing becomes a very challenging task in the vehicular networks [12]. More over the routed information's are often affected by variety security threats affecting the communication. Further, certain emergent situations such as the natural disasters, accidents, damaged roads, sudden break down of the vehicles and the appearance of the emergency vehicles still worsen the traffic scenarios and disturbs the communication causing delay in the transmission or failure in transmission affecting the safety and the leading to fatalities on road.

To ensure the safety of on road vehicles and elude the collision of the vehicles that take place due to improper communications or communication attacks, the paper puts forth an effective routing protocol with collision avoidance, (ERPCA) to identify vehicles with the reliability to transfer information on time and evade the discomforts in travelling. The paper is organized with the existing work in part 2, proposed work in part 3, result analysis in part 4 and conclusion in part 5

2. EXISTING WORK [5]

The existing vehicular network tries to enhance the security capabilities by developing a cloud-edge based roadside unit that is installed with an approximate member query filter to eliminate the request of the attack vehicles. The vehicles in the system is also aided with the on board unit that holds the approximate member query filter to be aware of the illegal access. This system allows the vehicles in the area to communicate only if its identity is revealed to the edge cloud. On revealing the identity of the vehicle receives a public key from the edge that is common for all the vehicles in the arena and verifies the key each time the information is conveyed. The vehicle that leaves the range is recorded in the database that maintains the entry and the exit list of the authorized vehicles. Though the existing the figure.2 below shows the step in the existing methodology to have a communication between the vehicles and the edge model.

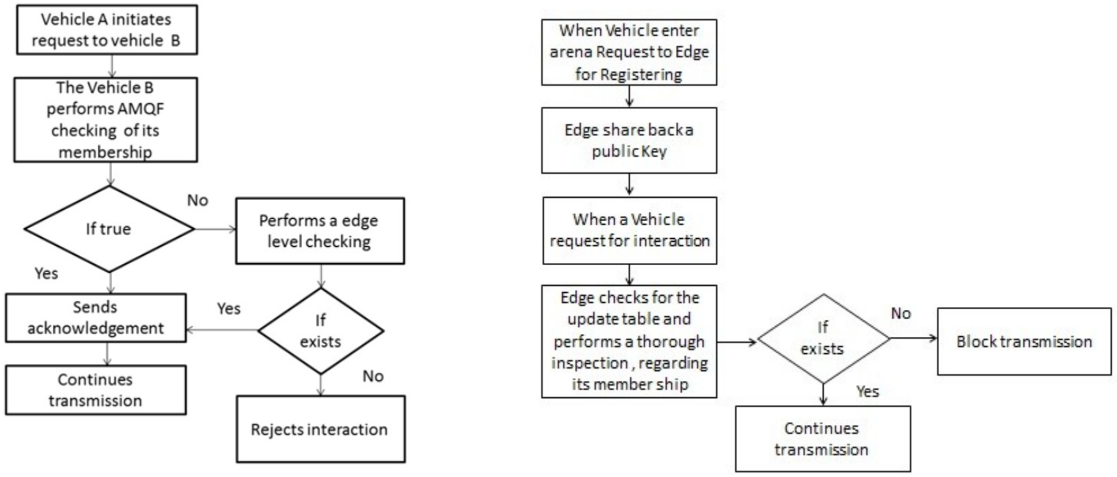

Vehicle A initiates request to vehicle B
The Vehicle B performs AMQF checking of its membership
If true
No
Performs a edge level checking
Yes
Sends acknowledgement
Yes
If exists
No
Continues transmission
Rejects interaction
When Vehicle enter arena Request to Edge for Registering
Edge share back a public Key
When a Vehicle request for interaction
Edge checks for the update table and performs a thorough inspection , regarding its member ship
If exists
No
Block transmission
Yes
Continues transmission

Fig.2 Existing VANET security [5]

Though very promising there are chances in which the even the attacking vehicles could reveal themselves as the normal vehicles and start communicating in the network affecting the actual communication and causing accidents and discomforts while travelling. This could further result in delay in the communication process affecting the throughput of the network and causing failure in information transmission.

3. PROPOSED WORK

The vehicular-adhoc network mainly scopes in improving the movement of the people and the goods. These networks obtain and procure an increasing attention due to the multitudes of the application supported by them. It provides the protection and convenience to the travelers and secures them from ill-fated incidents. The proposed process put forth in the paper aims at the improving the safety of the information transmitted on the emergent situations, by identify the reliable nodes with maximum residual energy. The flow chart below in fig. 3 expresses the phase in the proposed design.

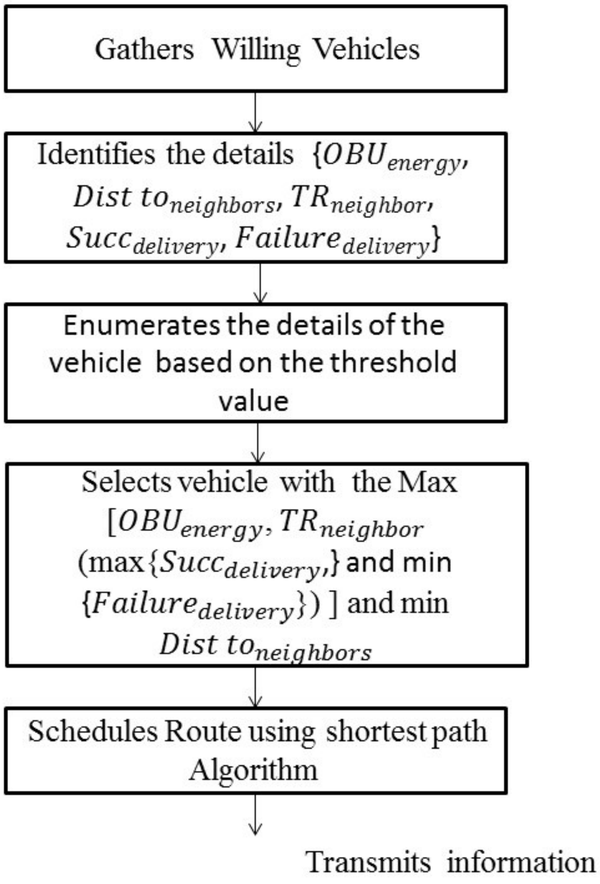
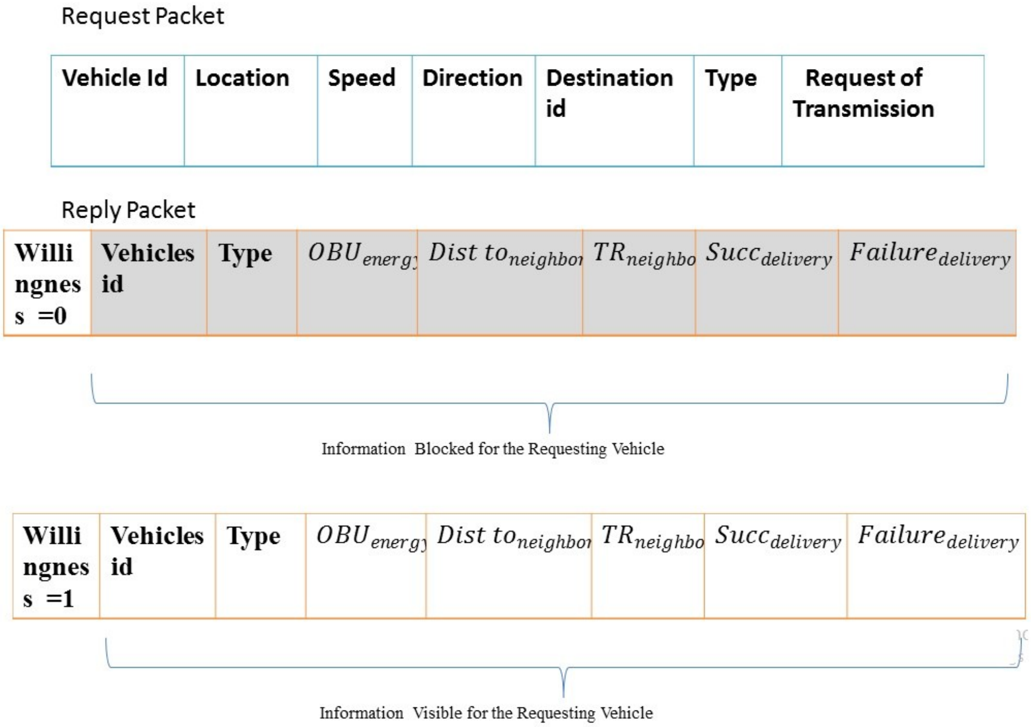

Gathers Willing Vehicles
Identifies the details $\{OBU_{energy}, Dist\ to_{neighbors}, TR_{neighbor}, Succ_{delivery}, Failure_{delivery}\}$
Enumerates the details of the vehicle based on the threshold value
Selects vehicle with the Max $[OBU_{energy}, TR_{neighbor}$ (max$\{Succ_{delivery},\}$ and min $\{Failure_{delivery}\})$] and min $Dist\ to_{neighbors}$
Schedules Route using shortest path Algorithm
Transmits information

Fig.3 Proposed Flow Chart

The paper aims in improving the convenience in the transportation for the during the certain emergency situations such as the accidents, vehicle break down, natural disasters, damaged roads, appearance of the emergency vehicles etc.

For a set of vehicles $\{v_1, v_2, v_3 \ldots\ldots\ldots\ldots. v_i\}$ within the communication range (C_r) of the road side unit(RSU)/ requesting vehicle $(Rqst_{Vehicle})$, periodic request are sent by the road side unit or the vehicle. The sensor equipped in the vehicles in the on board units help in recognizing the request signal and responds back to it if it is willing to take part in the network, the willing ness of the vehicle is send back with the reply highlight the willingness as column in the reply as the '0' if not willing and '1' if willing. The Fig. 4 shows the request and the reply packet.

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019)
Vol.01/ No. 02
Pages: 76-86
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2019.2.002



Request Packet

Vehicle Id	Location	Speed	Direction	Destination id	Type	Request of Transmission

Reply Packet

Willingness =0	Vehicles id	Type	OBU_{energ}	$Dist\ to_{neighbor}$	$TR_{neighbo}$	$Succ_{delivery}$	$Failure_{delivery}$

Information Blocked for the Requesting Vehicle

Willingness =1	Vehicles id	Type	OBU_{energ}	$Dist\ to_{neighbor}$	$TR_{neighbo}$	$Succ_{delivery}$	$Failure_{delivery}$

Information Visible for the Requesting Vehicle

Fig.4Request and the Reply Packet

The road side unit/vehicle on receiving the reply checks it to know the willingness of the vehicle, the details {energy the on board unit holds(OBU_{energy}), the distance to its neighboring vehicles ($Dist\ to_{neighbors}$), the trust report from its neighbor ($TR_{neighbor}$), details of number of data packets delivered safely ($Succ_{delivery}$) and the number of failures in the delivery($Failure_{delivery}$)) of the willing vehicle is collected. The table.1 provides the threshold set for each parameter.

OBU_{energy}	$Dist\ to_{neighbors}$	$TR_{neighbor}$
> 50% of original	< 1/3 of (source to destination distance)	Success rate = 80% and above Failure < 10 %

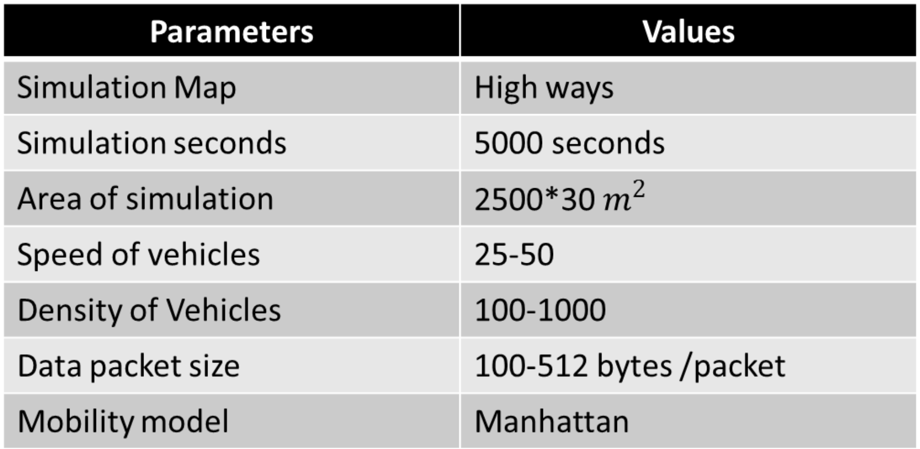
Table.1 Threshold level

The parameter gathered is compared with the threshold level set, to identify the optimal vehicles for the communication. All the vehicles that show interest in joining the network are enumerated one by one to identify the optimal set of vehicles that are closer by to extend communication. The routes are identified using the shortest path algorithm (Dijkstra's Algorithm), that ensures the path framed between each vehicle form the source to the destination and the intermediate vehicles are short.

The information's from the source to the destination vehicle is transmitted safely without any attacks and failures through the shortest path. The information's of the vehicles as well as the shortest route are periodically updated to the server by regularly sending request and collecting the vehicle details; this avoids the link failures and protects the lifetime of the network as vehicles with the maximum on board unit energy and the trust are joined to the network and the one with lesser energy level and trust than the threshold level are rejected from becoming the members of the network.

4. RESULT ANALYSIS

The ERPCA model is evaluated in the network simulator-2, to verify the transmission rate, the total number of successful deliveries and the total number of failures in transmission and spot out the capabilities of the ERPCA. The output is verified for the varying trust percentage of the vehicles and compared with the prevailing method that provides the security assistance for the VANET using the cloud computing [5], the table.2 Shows the parameters used in the simulation.



Parameters	Values
Simulation Map	High ways
Simulation seconds	5000 seconds
Area of simulation	2500*30 m^2
Speed of vehicles	25-50
Density of Vehicles	100-1000
Data packet size	100-512 bytes /packet
Mobility model	Manhattan

Table.2 Simulation Parameters and Values

The fig. 5 below provides the results of the transmission rate observed for the ERPCA and the security assistance for the VANET using the cloud computing, the transmission rate of ERPCA is found to be high compared to the other method during the emergency situations on road and further improves the convince and the safety in the transmission.

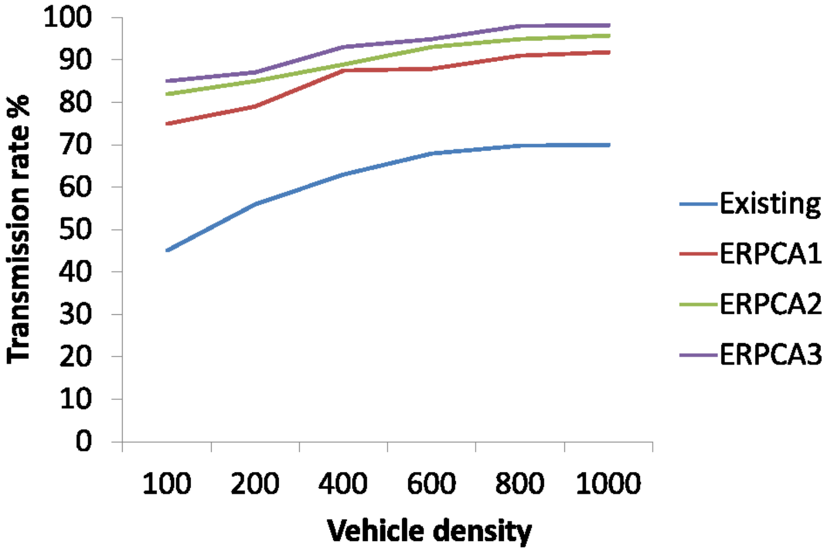


Fig.5 Transmission Rate

The fig.6 below provides the number of successful deliveries and failures in the vehicular network by employing the ERPCA for varying trust percentage of the vehicles joined in the network.

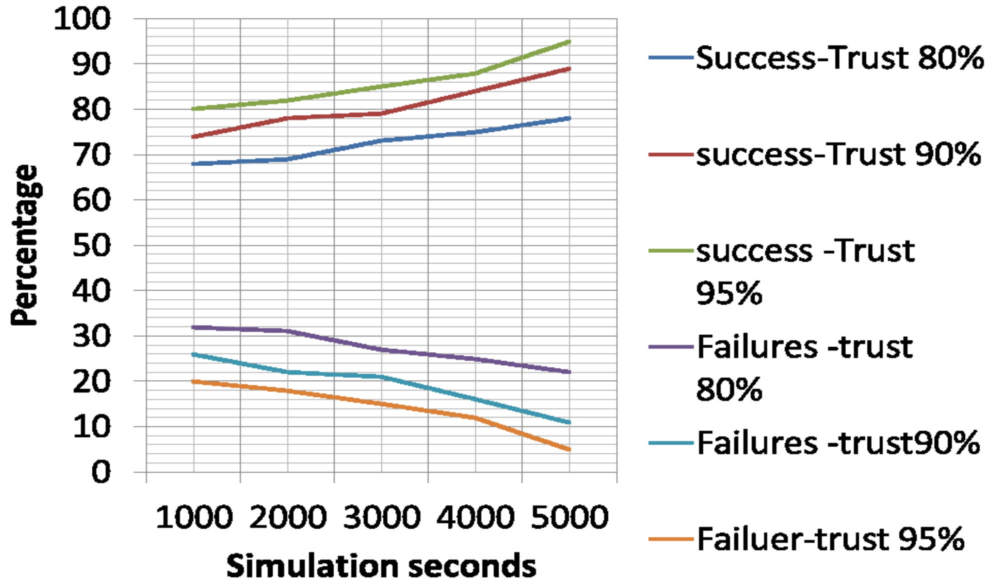


Fig.6 Successful deliveries and Failures Encountered by Employing ERPCA

The Table.3 below provides the observed output for the varying trust percentage of the vehicles and its comparison with the prevailing method that provides the security assistance for the VANET using the cloud computing.

Vehicle Density	Transmission Rate %		Successful Deliveries %		Failures in deliveries %		Energy consumption (joules)		Delay (ms)		Vehicles affected %	
	ERPCA	EXISTING	ERPCA	EXISTING	ERPCA	EXISTING	ERPCA	EXISTING	ERPCA	EXISTING	ERPCA	EXISTING
100	85	45	80	57	20	43	25	47	.0134	.1234	10	25
200	87	56	82	59	18	41	34	56	.0145	.1823	7	45
400	93	63	85	62	15	38	36	58	.0267	.23445	8	65
600	95	68	88	67	12	33	45	64	.0346	.5678	4	78
800	98	69.89	95	68	5	32	47	68	.04567	.678	5	95
1000	98.2	70	98	74	2	26	50	75	.0567	.7632	3	100

Table.3 Comparison Table

5. CONCLUSION

The work carried out in the paper has successfully framed an efficient routing protocol with the collision avoidance to enhance the fluency in the traffic as well as convince in the travelling. The proposed methodology ensures the maximum successful deliveries of the information's from the source to the destination by identify the trusted vehicles with maximum energy level and minimum distance to the destination. This enables the vehicles to avoid getting piled up in the emergency situations on road. The ERPCA allows the safe and comfortable travelling, the results obtained based on the transmission rate, successful deliveries, failures, energy consumption and the delay in the transmission proves the capability of the proposed ERPCA and its comparison with the existing security assistance for the VANET using the cloud computing shows that the ERPCA has 20% higher transmission rate compared to the prevailing method.

References

[1] Bhalaji, N. "PERFORMANCE EVALUATION OF FLYING WIRELESS NETWORK WITH VANET ROUTING PROTOCOL." *Journal of ISMAC* 1, no. 01 (2019): 56-71.

[2] Pandian, M. Durai. "ENHANCED NETWORK SELECTION AND HANDOVER SCHEMA FOR HETEROGENEOUS WIRELESS NETWORKS." *Journal of ISMAC* 1, no. 03 (2019): 160-171.

[3] Smys, S., and Jennifer S. Raj. "A STOCHASTIC MOBILE DATA TRAFFIC MODEL FOR VEHICULAR AD HOC NETWORKS." *Journal of Ubiquitous Computing and Communication Technologies (UCCT)* 1, no. 01 (2019): 55-63.

[4] Duraipandian, M. "PERFORMANCE EVALUATION OF ROUTING ALGORITHM FOR MANET BASED ON THE MACHINE LEARNING TECHNIQUES." *Journal of trends in Computer Science and Smart technology (TCSST)* 1, no. 01 (2019): 25-38.

[5] Neelaveni, R. "PERFORMANCE ENHANCEMENT AND SECURITY ASSISTANCE FOR VANET USING CLOUD COMPUTING." *Journal of trends in Computer Science and Smart technology (TCSST)* 1, no. 01 (2019): 39-50.

[6] Bhalaji, N. "QOS AND DEFENSE ENHANCEMENT USING BLOCK CHAIN FOR FLY WIRELESS NETWORKS." *Journal of trends in Computer Science and Smart technology (TCSST)* 1, no. 01 (2019): 1-13..

[7] Haoxiang, Wang, and S. Smys. "QOS ENHANCED ROUTING PROTOCOLS FOR VEHICULAR NETWORK USING SOFT COMPUTING TECHNIQUE." *Journal of Soft Computing Paradigm (JSCP)* 1, no. 02 (2019): 91-102.

[8] Koresh, Mr H. James Deva. "COMPUTER VISION BASED TRAFFIC SIGN SENSING FOR SMART TRANSPORT." *Journal of Innovative Image Processing (JIIP)* 1, no. 01 (2019): 11-19.

[9] Smys, S., Jennifer S. Raj, and Nixon Augustine. "AUTONOUMOUS VEHICLE NAVIGATION IN COMMUNICATION CHALLENGED ENVIRONMENTS-A SIMULATION APPROACH." (2011).

[10] Raj, Jennifer S., and A. Anto Prem Kumar. "ENERGY EFFICIENT LOCALIZATION AND ROUTING STRATEGY FOR CLUSTER BASED SENSOR NETWORKS."

[11] Ananthi, J. Vijitha, and Jennifer S. Raj. "A Peer to Peer Overlay Approach for Topology Maintenance in Wireless Networks."

[12] Smys, S., Hui-Ming Wee, and Meng Joo. "Introduction to the Special Section on Inventive Systems and Smart Cities." (2018): 32-33.