Optimization Based Trust Classification for Safe and Secured Communication in Vanet

Mr. Mohammed Sirajudheen A,
Part Time Research Scholar - Department of Electronics and Communication Engineering, Karunya Institute of Technology and Sciences Coimbatore – 641114.

Dr. D. Jasmine David,
Assistant Professor - Department of Electronics and Communication Engineering, Karunya Institute of Technology and Sciences, Coimbatore – 641114.

ABSTRACT

A vital communications system for transferring messages for any situation on the road is Vehicle Ad Hoc Networks (VANETs). In VANET, it was difficult to solve the conundrum of choosing the safest, most efficient path. Therefore, the safest and most dependable route will provide the best answer to the routing problems in the VANET. The efficient, safest route is quickly found in this paper by applying the Multi-Objective Bio-inspired Heuristic Cuckoo Search Node optimisation technique. Using the Stochastic Discriminant Random Forest Node Classifier, the node can be discriminated based on traffic and security after being shown an optimal route.

Keywords: Vehicle Ad Hoc Networks, the Trust Aware extreme Gradient Boosting Node Classification algorithm, the Stochastic Discriminant Random Forest Node Classifier, the Multi-Objective Bio-inspired Heuristic Cuckoo Search Node Optimisation algorithm, and the Weighted End-to-End Delay-Based Approach.

1.INTRODUCTION

Networks ad-hoc for vehicles has built interest in remote goods which are directly available to vehicles. Other functions include remote keyless devices for passageways, workstations, PDAs and mobile telephones. The value of the Vehicle-to-Vehicle, Vehicle-to-Road, and Vehicle-to-Infrastructure (V2I) interaction continues to develop as mobile remote devices and systems. The VANET is a modern demanding network system seeking an all-embracing networking paradigm for the future. The creative structure of ad hoc mobile networks (MANET) which communicate between vehicles. This can be thought of as each vehicle is equipped with an ad-hoc network connectivity wireless communication facility. Every vehicle in the network.

Will transmit, receive, and distribute messages to other vehicles in the network, continuing to run without infrastructure. This enables vehicles to exchange information in real-time, and road conditions and other travel-related information are available for drivers to be informed. In the last few years, many research work investigating various problems found with the V2I, V2V and V2R sectors, taking a key role in the IT fields In fact, in the last decade or many governments companies and academic organizations worldwide have updated various VANET project. In vehicular communication, Road traffic plays an important role. The transportation system today has now become an indispensable, comprehensive part of daily human life. On average, 45% of transit users are estimated to spend one hour.

In recent years, the greater the number of people depending on the transport system. In order to improve transport systems safety and efficiency, several innovative services regarding transport and traffic management were developed. It helps drivers to be better informed and to make safer and more organized decisions on the lane. Vehicles transmit information to another automobile and connect to each alternative. The inter-vehicle communication arrangement transfer and receive the traffic-related data over numerous hops to a multiple of recipients. In VANET, communication is developed for sharing the information about the road conditions and traffic in order to prevent road accidents and efficient information about the traffic. During communication, Spam messages could be distributed by the malicious node to render such stuff as false data will lead to crashes, theft and heavy traffic. VANET's safety is important since its quality has to do with hazardous conditions.

The critical information should be accessed by a malicious party or changed. The system will most likely determine the responsibility of the driver while ensuring his health. According to the calculation of the device, velocity and unintended relation between the vehicles, the relative geographical area they provide an adequate figure and power assets on their typical systems. There will be a growing number of vehicles now a day. Therefore, traffic security and motion obstruction should be extended. To overcome the in this work, an innovative strategy was put into practice to address VANET-related challenges. The essay could be organized as follows: The quick overview of routing and security challenges in the VANET is shown in Section 1. The several more approaches already in use to address VANET-related problems, as shown in Section 2. The challenge in VANET is then presented in Section 3. Section 4 provided an explanation of the investigation of the suggested approach. Finally, the simulation's outcomes and conclusions were looked at.

2. LITERATURE SURVEY

Tomar et al. [1] identified the issue of a hidden using the NS-2 tool in vehicle nodes, terminal. also examined vehicle communication reliability in the small communication distance and increased throughput among the various nodes in the VANET framework using the NetSim tool during communication. Loganathan et al. [2] proposed the warning administration to prevent malfunctions through warning drivers about malfunctions and dangerous conditions on the road. This policy contains the sense of another dispersal method of contact. A road condition in VANET is tested in order to evaluate how well-being strategies minimize the reaction time of the operator in an incredible scenario. Karimzadeh et al. [3] described that only the related cars which are expected to travel through crash areas could get a traffic safety alert, like the incident notices. Accessible to the vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) or hybrid networking is used for the delivery of a signal to the related vehicles according to network connectivity. By using VANET mobility data sets, the implemented system was evaluated. Koti et al. [4] For vehicle to vehicle (V-V) communication, a multi-agent based safety information distribution strategy has been developed. We have chosen a few far-end nodes in outer range for information delivery in the suggested dissemination method, resulting in a lower number of transmissions. . Jose et al. [5] Planned multi-agent centred vehicle-to-vehicle contact safety information distribution scheme(V-V). They also employed the collection of existing nodes for the delivery of data with a decreased transmitting number in the planned distribution scheme. Nguyen et al. [6] Cooperative System for retransmitting security packets that were not sent by secret nodes. The simulation's results demonstrate that RAM not only improves the efficiency of security packet distribution using current MAC protocols but also supersedes them in terms of protection and control packet distribution. delivery ratios. Tomar et al. [7] suggested a way of using RSU to calculate the vehicle's contact distance for different routes. RSU has been spread in clusters. The approach based on security controls and the theory was proposed in this article. based on each map's performance, the current time, average time, travel speed, driving distance, and average,, was evaluated the outcomes of three different maps. Li et al. [8] To reduce congestion and keep the channel contained, the congestion control framework for adaptive beacon generation (ABGR) was presented. In order to ensure that the beacons are transmitted precisely and on time, the beacon generating frequency can be gradually changed in accordance with various vehicle volume rates. It was suggested to use the dynamic application-level quality testing technique (T-Pro) to assess how well various security systems work at various densities. The emphasis is on comparing traffic density and speed. Finally, the applicability consistency of three security systems was evaluated using the approach ABGR.

Naja et al. [9] proposed a new approach to evaluate the volume of interference of a network depending on a vehicle speed throughout the hope of time-waiting of contra-based and probability-based schemes. Simulation tests via NS2 with 802.11P indicate that under various scenarios, the new approach works far better. Benkirane et al. [10] by using the RSUs distributed and collaborative technique to pinpoint Sybil's vehicles on the basis of their real positions, they proposing an appropriate solution with this serious threat.Cui et al. [11] Propose an effective VANET semi trusted authority encryption scheme In that they incorporate the approach of self-healing key delivery in a semi-trusted authority setting with a certificate-free signature so that CRLs are not demanded from the beneficiaries.

Ramakrishnan et al. [12] Cuckoo search algorithm (ARP-CS) adaptive routing protocol design proposal. The adaptive protocol combines the capability of topology and geographical protocols, ensuring secure data transmission in a short amount of time with a high packet delivery rate. For authenticating both the network level and the node level against, Erskine et al. [13] developed a fog computation (FC), which includes the CUC, the firefly algorithm (FA), the fire-fly neural network, and a key-distribution (KDE) facility. any trustworthiness assault in VANET, in the context of the hybrid optimization algorithms (OAs). The proposed scheme is referred to as the "Fog Computing Secure Intelligent Vehicle Network" (SIVNFC).

As a classification tool to distinguish between actual vehicles and fighting vehicles, a feedback neural propagation network (FFBP-NN), often called a firefly neural network, is used. Limbasiya et al. [14] can address the current issues on the VANET and suggest using the batch validation (ESCBV) protocol, a communication method that is both secure and efficient..(Mazilu, Teler et al. 2011).[15]The bandwidth limited in the existing work. The new protocol used to implement good data security, good data management, reduce the secure the attacks and also improve the efficiency with the help of high storage capacity.(Jaballah, Conti et al. 2020)state of the art SDN based adhoc network structure for the network design, specification and the main purpose can be consider to implement the secure network. That required improving the future Intelligent Transportation systems. (Jenefa .F et al.2017)This proposed vehicular network is used reduced the latency in the cellular network. It can be determine the combination of vehicle and roadside. The proposed method is used to increase level in the network. The inter vehicle communication can be done between the RSU and the vehicle.

To implement the well known communication level in the communication by the use of RSA algorithm. (SathyaNarayanan 2019)It is similar to the previous paper the implementation can be done due to the secure level in the communication between the road sides units as well as vehicle here use the WAVE protocol and it also improve the efficiency level good in the communication with the help of SSVC mechanism. When compare to the existing protocol. (Yiliang, Xi et al. 2017)The communication between the both RSU and vehicle it mainly focused the privacy information can be affected due to the privacy. They also secure the accident and reliability in this paper and also secure the combine group signatures and IBSC.

3. PROBLEM STATEMENT

The characteristics of attacks and some threats can be occurring in the network. The communication between the RSU as well as traffic in the environment. Due to the communication does not provide the efficient manner. The affecting factors are high rates, the network connection, communications among the RSU terminal, flexibility the proposed (**TAXGBNC-SR**) protocol is used to rectify the problem. And it should be more secure communication and make it very flexible node in the VANET. They efficiently provide the effective way to detect the routing issues in the VANET is required to manage the secure communication.

4. PROPOSED METHODOLOGY

The suggested technique locates the ideal path to a source and uses that path to relay the message. To choose the best path, it employs the multi-objective, biologically inspired heuristic cuckoo search optimisation method. The procedures depicted and also identified the node and the implementation can be shown in the figure 1.

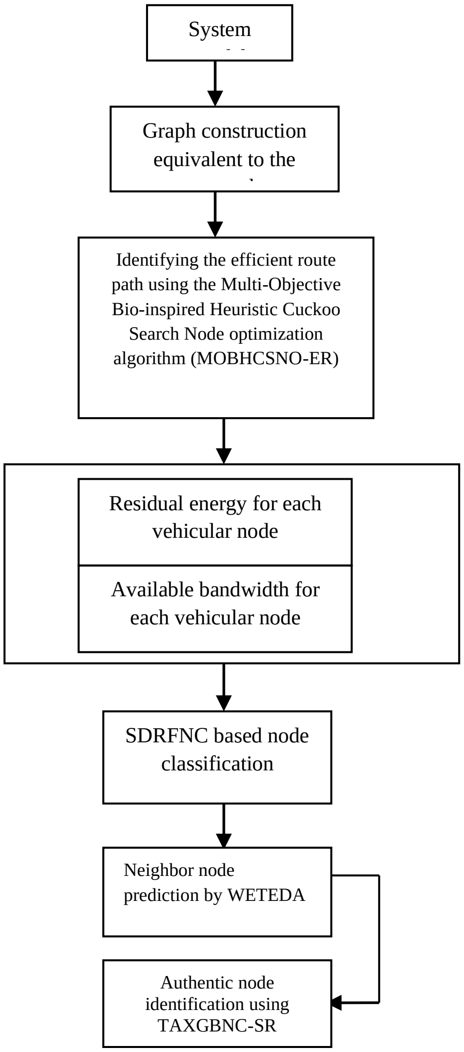

System
Graph construction equivalent to the
Identifying the efficient route path using the Multi-Objective Bio-inspired Heuristic Cuckoo Search Node optimization algorithm (MOBHCSNO-ER)
Residual energy for each vehicular node
Available bandwidth for each vehicular node
SDRFNC based node classification
Neighbor node prediction by WETEDA
Authentic node identification using TAXGBNC-SR

Figure: 1 schematic representation of the proposed method

4.1 System model

The optimum paths between the source and the destination are chosen using the VANET model under the following presumptions. Message alerts, driving forecasts, and information services are just a few of the unique services that the routing in the network offers to its clients. The road network has played a crucial role in many ITS-related applications, including brake warning, weather forecasting, traffic, vehicle safety, and driver safety. Therefore, there is a critical need for a vehicle-to-vehicle communication system that is trustworthy, stable, and qualified to deliver a security message when necessary. The implementation and design of the road network have undergone numerous attempts to be standardized. The network model that should be taken into account when building the structure of the road model. Let N be the average number of network cars, which will be 2. There will be 2 vehicles each segment. Here, the origin is informed about the destination path through our route discovery procedure. After being gathered, the data is sent in that direction by the information source. In this, the source vehicle selected the finest neighbourhood. Consequently, the optimisation method was employed to select the safest route free of traffic.

4.2 Multi-objective bio-inspired heuristic cuckoo search node optimization-based efficient routing

In VANET routing, estimating traffic between the source and destination locations is typically the optimal method of route selection. As a high traffic density increases the flow of vehicles on the road, the direction of a low traffic density is preferred for the best route selection. Therefore, an active prediction system is required for selecting the optimum path. The main step of the currently used strategy is route investigation. The optimal path, taking into account all the various restrictions, is found by the optimisation method from source to destination. An algorithm can be used to optimize multipath and produce trustworthy data.. If the nodes are not energy-efficient and are overloaded due to excessive traffic, the data transfer to the destination may be delayed during the route selection process. MOBHCSNO-ER algorithm is therefore suggested for routing optimisation. The suggested algorithm selects the most effective multipath routing to deliver the information quickly. The settings must be initialized in order for route detection to be effective. Calculating the nest size and the mutation probability is necessary to set the upper and lower band parameters. Choosing the right nest is essential,

$$\beta = \beta_{max}\text{-}(N_{iter}/N_{iter(total)}{}^{*}\beta_{max} - \beta_{min} \qquad (1)$$

Where N_iter stands for the current iteration number and N_(iter(total)) for the total iteration number, respectively, while _max and _min indicate the maximum and smallest nest size. The nest size will decrease as the iteration count rises, as represented in equation (1). Mutation probability is connected to fitness according to the MOBHCSNO-ER algorithm.

$$P_f(\mathrm{i})=\begin{cases} P_{f_{min}} + \left(P_{f_{max}} - P_{f_{min}}\right) * K, K < 1 \\ P_{f_{max}/}N_{iter}, \end{cases} \mathrm{i=1...n} \quad (2)$$

where f= fitness(i) − f_{min}, which is dependent on the current state of the ith solution; fitness(i) and fmin stand for the current state of the ith solution and the current state of the population's global optimal fitness, respectively; P_(f_max) and P_(f_min) stand for the maximum and minimum of the mutation probability Pa, respectively. It is clear from equation 2 that the fitness of the solution is modified, as well as the mutation probability, which is proportional to K. Generally speaking, the mutation probability varies according to the number of iterations. The nest position is examined after the parameter is initialized.σ_v=($\boldsymbol{\gamma}$(1+β_p))*sin($\boldsymbol{\pi}$*β_p/ 2)/($\boldsymbol{\gamma}$(1+β_p 2)* ${\beta_p}^{\beta_p - 1/2}$)* $(\beta_p - 1/2)^{1/(\beta_p - 1/2)}$ (3)

where _v denotes the nest's arbitrary size.

The revised version of equation (3) is,

n_p = rand(_san,1)*(u_b-l_b) + l_b (4)

where n_p denotes the nest's arbitrary location.

The objective function must then be calculated in order to determine the closest node path. Node localization's goal is to infer the unknown nodes' coordinates from the anchor vehicular nodes. Each unknown node can be calculated separately from its anchor .

$$\sigma^{2} = \gamma^2 * e_{ij^2} \qquad (5)$$

Where e_(ij1) is the original distance of the unknown node and 2 is the error variance. The standard deviation was proportional to the error variance, as can be seen from equation (5). Equation (6) was used to represent the measured separation between the anchor node and the unknown distance node.

$$e_{ij'} = e_{ij} + N_{ij} \qquad (6)$$

N_ij stands for the mistake of the unidentified vehicular node. The goal function, which represents the mean error of the unknown node and the anchor nodes combined, should then be determined.

$$f(x_i y_i)=\frac{1}{n}\sum_{j=1}^{n}(e_{ij} - e_{ij'})\text{^}2 \qquad (7)$$

The MOBHCSNO-ER technique can be used to estimate the unknown vehicular node's coordinates. When the objective function is minimised, it suggests that it was simple to estimate the unknown short-distance path node.

$$obj_{fn}=-20*\exp(-2*\sqrt{\sum \sigma_v})/2-\exp(\sum \cos(2\pi * \sigma_v)/d_b)+20\exp(1) \qquad (8)$$

The positions of alpha, beta, and gamma are then updated. It can be updated to reveal the path. Multiple paths will then be transmitted to the source as part of the route response that is sent from the destination. Each node's load, remaining energy, and hop count are all included in the reply packet. After that, the origin node studies the answer packets it received via various routes to assess the fitness of each one. the n path locations that select the n number of paths and the highest level of fitness. The routing table of the source node has each path's fitness values listed in descending order according to the data transmitted along each path. Regardless of success or failure, the next best fitness value path transmits the data. If any of the n paths experience communication difficulties, the algorithm is then discovered and the process is repeated. The routing table is adjusted by attaching all of the aforementioned metrics in accordance with the reverse path defined by dragging them up until the recipient vehicle node is hit if RRPLY sends to the neighbour node via destination node until the sender node that reaches. Applying the aforementioned algorithm now determines the fitness value at the sender vehicular node. The routing table's descending order and the data that will be stored in descending order. As of right now, the sender vehicular node actually starts transmitting data using the path with the highest fitness value in its routing database. If that path fails, the sender uses the second-best fitness path, and so on. Where F is the fitness score assigned to every path that the source node has received and identified. Here, the bandwidth distance between each pair of nodes and the residual energy between each node may both be computed. Fitness is assessed using energy, metric delay, and shortest route. The answer to the suggested methodology is given below. The data packet sent by the source vehicular node is represented by the cuckoo in this instance and the cuckoo's egg. Here, the data packets and the vehicle source are conveyed via a multi-objective path that can reach the destination node. Dropouts occur when data is transmitted along a busy path or over an unstable power source.

Algorithm 1 (MOBHCSNO- ER)

```
Input:   Vehicle Node $V_n$,Node_coordinate $V_c$,bound limit $V_{x,}V_y$, energy parameter $V_{e,}$
Output: Optimized valued $\varphi_p$ and $\gamma_i$ (best nest and route path)
Step1: initialize the parameters,
        [ $V_{x,}V_y$]=[Upper Limit lower limit]
          Max_iteration $max_{iter}$=100;
Lower band $l_b$=$V_x$ (1)*($V_c$, 2);
Upper band $u_b$=max($V_c$, 2)
best near $n_b$ Dimensions $d_b$=size($u_b$, 2)
Step 2: initialize the nest position $n_p$,
N=size ($n_p$)
        beta_pos $\beta_p$=3/2;
$\sigma_v$=($\gamma$(1+$\beta_p$))*sin($\pi$*$\beta_p$/2)/($\gamma$(1+$\beta_p$/2)* $\beta_p^{\beta_p-1/2}$)* $(\beta_p-1/2)^{1/(\beta_p-1/2)}$
for j=1:n
  s=$n_p$(j,:)
u=randn(size(s)* $\sigma_v$)
v=rand(size(s))
 Let compute nest  position ,$n_p$=rand($\tau_{san}$,1)*( $u_b - l_b$)+ $l_b$
step 3: calculate objective function,
to compute best near nest position,
        for jj=1:size($n_p$)
                for i=1:size($pos_{data}$, 1)+
)* $\beta_p^{\beta_p-1/2}$)* $(\beta_p-1/2)^{1/(\beta_p-1/2)}$
                  flag4ub=$pos_{data}$(I,:)> $u_b$
                    flag4lb=$pos_{data}$(I,:)< $l_b$
                     $pos_{data}$(I,:)= $pos_{data}(i,:)$*(

   $d_b$=size(PI,2)
    $obj_{fn}$=-20*exp(-2*$\sqrt{\sum \sigma_v}$)/2-exp($\sum cos$ $(2\pi * \sigma_v)/d_b$)+20exp                    (1)

Step 4: Update the alpha, beta and delta positions,
      If $obj_{fn}$<$\alpha_p$
      $\alpha_p = obj_{fn}$
   $\alpha_p$=$pos_{data}$(I,:)
End
If $obj_{fn}$<$\alpha_p$ && $obj_{fn}$<$\beta_p$
 $\beta_p$=$obj_{fn}$
End
If  $obj_{fn}$<$\alpha_p$ && $obj_{fn} > \beta_p$ && $obj_{fn}$<$\gamma_p$
$\gamma_p$=$obj_{fn}$
End
 end
end
```

4.3 Stochastic discriminant random forest Node classification

Statistical discriminant The supervised method Random Forest divides the class with the most votes in each of the classes of the trees into a subset of features at the exercise. Simply said, this supervised learning approach is superior to others. First, it may be applied to guarantee high precision in both identification and regression tasks. Second, the overcrowding of trees in the design is prohibited if more trees grow. It is capable of handling a huge, more extensive data array.. Eventually, the SDRF node classifier will be able to handle missing values with the reliability of a significant fraction of the data. Each categorization algorithm will yield correct results when used independently. Even so, the performance of IDS can be enhanced by the combined implementation of these techniques. Analyzing various approaches has always been done to determine whether or not categorization outcomes could be improved. Then, using the model to distinguish between traffic and the authenticate route, we begin the categorization process. The stochastic discriminant Random Forest classifier is what we are employing for this. It is simple to calculate the trustworthy value. classifies a thing into a specific class by a majority vote of its neighbours. Using a learning dataset, the Random Forest Classifier creates a set of randomly chosen decision-making zones. This selects the final test entity category by combining the votes of various Decision Trees into a single word. The distance must be computed in order to determine the trustworthy categorised value.

$$\text{Distance(i,j)}=\sqrt{(V_{n_{fea}}(i,1)\text{-}V_{n_{fea}}(j-}\ 1))+(V_{n_{fea}}(i,1)-(V_{n_{fea}}(j,1)^2 \quad (9)$$

The prototypes were trained on typical car features and behaviour. Equation (10) can be used to calculate the vehicular node attributes in this situation.

$$V_{n\_fea}=[V_{n\_fea}\ \text{Distance}] \quad (10)$$

As a result, the classifier can assess the characteristics of the vehicular nodes and distinguish between the genuine node and the node with less traffic. The vehicle node's trust value was then determined.

$$V_{tv}=(V_{n\_fea}\ dist) \quad (11)$$

where the vehicular node's trusted value is represented by V_tv. The trusted value will determine how to identify the genuine node.

Algorithm:2 (Stochastic Discriminant Random Forest Node Classifier)

```
Input:   Vehicle Node features $V_{n\_fea}$,Node_coordinate $V_c$
Output: classified  valued $c_v$
To compute trust value,
For i=1:size($V_{n\_fea}$,1)
  For j=1:size($V_{n\_fea}$, 1)
        Distance(i,j)= $\sqrt{(V_{n_{fea}}(i,1)\text{-}V_{n_{fea}}(j-}$
$1))+(V_{n_{fea}}(i,1)-(V_{n_{fea}}(j,1)^2$
End
End
Vehicle Node features  $V_{n\_fea}$=[$V_{n\_fea}$ $Distance$]
To compute, trust value $V_{tv}$= ($V_{n\_fea}$ $dist$)
Class label=unique(target)
K=length(class label)
For i=1:k
 Temp=totalclassmean(I,:)
W(I,j)=-0.5* Temp* totalclassmean+log(i)
W(I,2:end)=temp
End
```

4.4 TAXGBNC-SR Routing prediction

By identifying the trusted value, the routing prediction may also be performed using the alternative trust-aware extreme gradient boosting node classification-based secured routing (TAXGBNC-SR) technique. In a manner similar to the (SDRFNC) method, (TAXGBNC-SR) may quickly identify the genuine node by using the trust value. In a variety of machine learning tasks, such as multi-class classification, learning to rank, and click prediction, TAXGBNC-SR achieves the most cutting-edge results. Due to the rise of big data recently, both the number of features and the number of instances,

More difficulties are being encountered by TAXGBNC-SR in terms of efficiency, accuracy, and data transfer. From this point on, the computational complexity will increase as the number of characteristics and instances increases. By lowering the amount of features and instances, an Efficient TAXGBNC-SR is created in this study to address the time-consuming issue. However, this is a fairly simple procedure. This research focuses on data sampling throughout the boosting process according to data weight and gearbox speed. This method may easily target both normal and pathological features after being applied straight along clusters. The formula can then be used to quickly identify the genuine node. V_{tv}= ($V_{n\_fea}\, dist$) (12)Just the other suggested route categorization approach is compared to this one. Then, a suggestion for the subsequent step that performed the best was made

```
.Algorithm:3(TAXGBNC-SR)
Input:   data features  $d_{n\_fea}$,data_class $d_c$
Output: classified  results $c_{res}$
To compute training deatures,
For ii=1:length($d_{n\_fea}$, $d_c$)
Rec=[-80 -80 80+$d_{n\_fea}$]
Y=rec(1)+rec(1)+81+rec(3);
End
To compute test data and trained data,

To compute, trust value $V_{tv}$= ($V_{n\_fea}$ $dist$)
Class label=unique(target)
Ang=ranprm=size($d_{n_{fea}}$,1)
$c_{res}$ =[datafeatues (ang,:)]
```

4.5 Weighed end to end delay approach based neighbor node prediction

The weighed end-to-end delay technique was made possible by the identification of the trusted Neighbour node. Both the packets used to pass the data and the hop-based latency were impacted. According to how long of a hop there is between the two with respect to time, the source and destination are always shifting.

The distance travelled that directly relates to the packet delay from end to end. If the path length increases, the end-to-end packet latency likewise grows. If there will be a strong bonding between them, it will be possible to determine the path length and packet delay. In the suggested weighed end-to-end delay strategy, the shortest path between each node and the source is estimated together with the weighted length of each path. The legitimate node is the weighed node, which is the node with the shortest distance, no link breaks, and the least amount of traffic. After receiving node information, the packets can be sent directly to the destination node. The practice of saving time also saves energy. The message is routinely disseminated throughout the network by that specific node. Each node updates its local tables after receiving messages. According on the signals it receives from its Neighbour, the focus node regularly modifies its locally maintained Neighbour Table. Using related information, it was possible to estimate the neighboring nodes' approximate bandwidth and relation lifespan. The data can be sent immediately from the source vehicular node to the destination node after determining the shortest, least congested path.

5. RESULTS AND DISUSSION

This section carefully examined how the suggested methods performed..

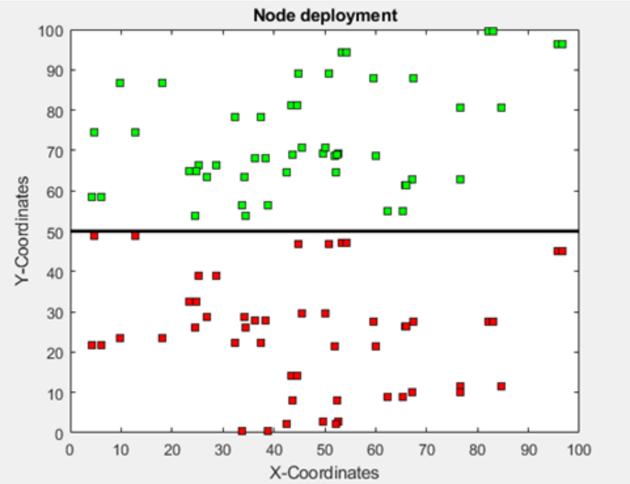


Figure: 2 Implemented system model

The node pair can be anticipated here to initiate the process, as seen in figure 3.

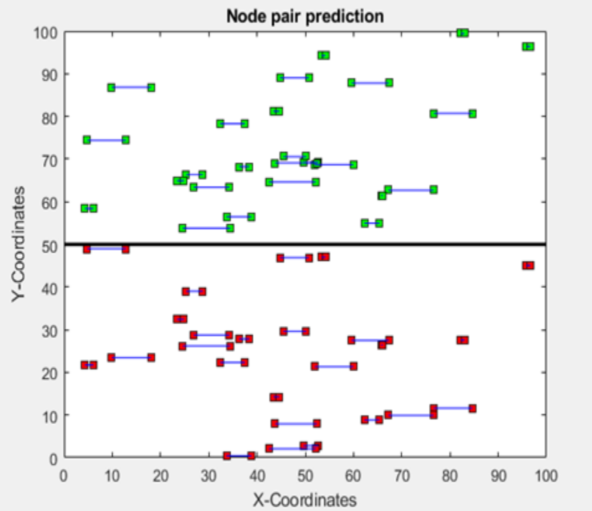


Figure: 3 Node pair prediction

The Neighbour route can then be built using one of three techniques following the node prediction. Figure 4 illustrates effective routing achieved utilizing the multi-objective, bio-inspired heuristic cuckoo search node optimisation. Here, the bandwidth distance between each pair of nodes and the residual energy between each node may both be computed.

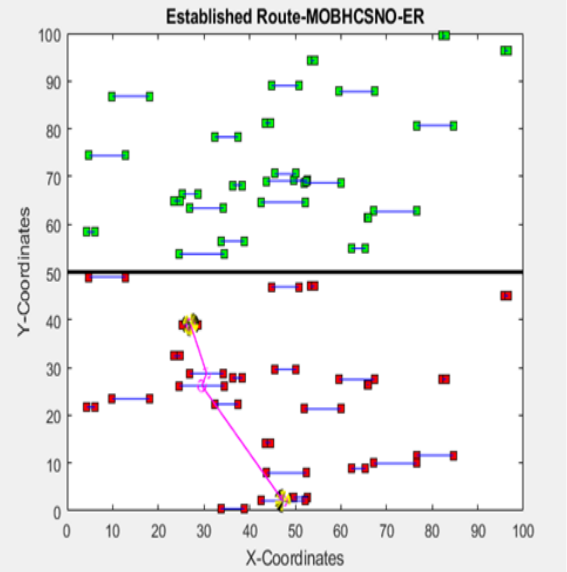


Figure: 4 Established route MOBHCSNO- ER

Following route establishment, it must be determined whether or not it is the safest shortest path. Figures 5 and 6 illustrate how the Stochastic Discriminant Random Forest Node Classifier and TAXGBNC-SR decision making model were used to determine the safest route.

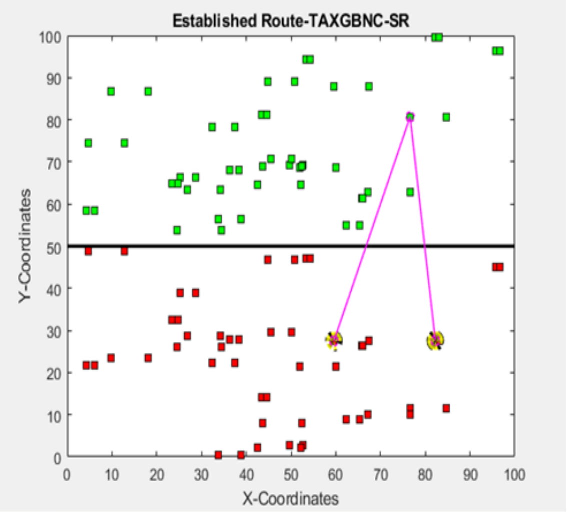


Figure: 5 Established route of TAXGBNC-SR

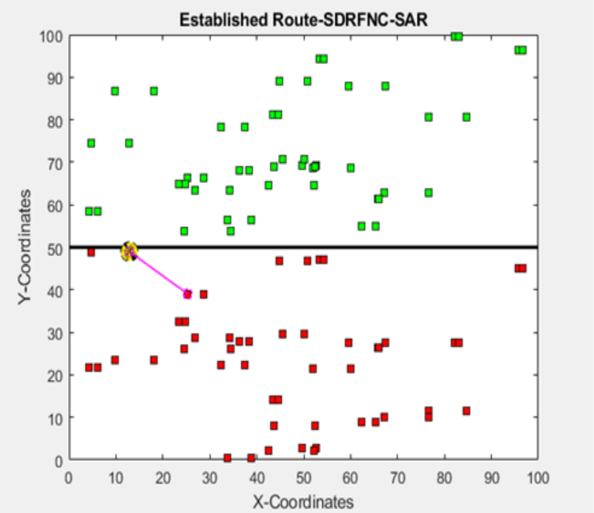


Figure: 6 Established route of Stochastic Discriminant Random Forest Node Classifier

5.1 Performance metrics

Stochastic Discriminant Random Forest Node Classifier will provide the quickest and safest route when compared to the TAXGBNC-SR when comparing the two decision-making techniques. **Throughput:**

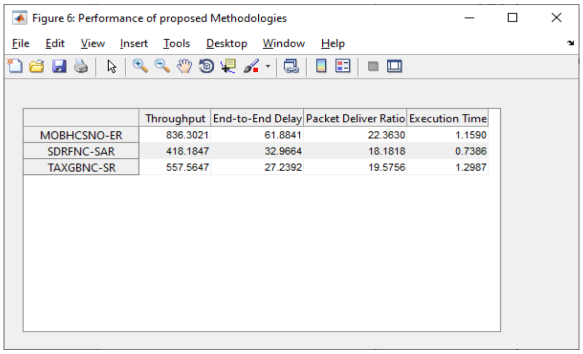
The amount of information efficiently transferred in a single attempt throughout the communication process Average end-to-end delay: It is possible to compute the pace at which time will be used for the entire transmitting process and the overall delay of messages being transmitted.

$$AD = (Ps-Pr) / Pr \qquad (13)$$

In this case, Ps stands for the packet sending time and Pr for the packet receiving time. The packet delivery ratio, in general, is the ratio of the volume of packets that can be transferred by the sender to the volume of packets that can be received by the sender.

. $$P = (Pr / Ps) *100 \qquad (14)$$

Here, P stands for packet delivery ratio, Pr for packet volume received, and Ps for packet volume sent. Figures 7 and 8 provide the performance comparison study of the suggested methods.



	Throughput	End-to-End Delay	Packet Deliver Ratio	Execution Time
MOBHCSNO-ER	836.3021	61.8841	22.3630	1.1590
SDRFNC-SAR	418.1847	32.9664	18.1818	0.7386
TAXGBNC-SR	557.5647	27.2392	19.5756	1.2987

Figure: 7 comparative analysis

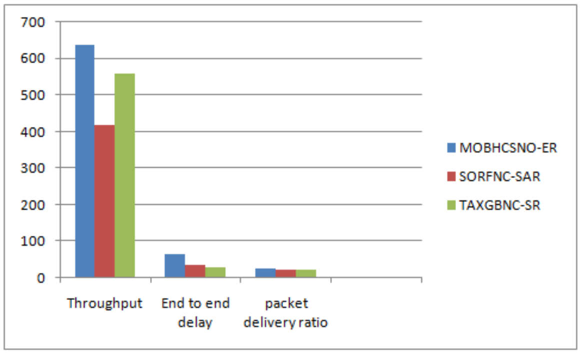


Figure: 8 performance comparative analysis

5.2 Comparative Analysis

By comparing the followed three approaches for the communication process, the traffic and its risk to be categorized according to their performance of the optimization and classification. The analysis to be given as, Multi-Objective Bio-inspired Heuristic Cuckoo Search Node optimization algorithm – Improved the road safety and the productivity of the transportation. This system may leads to the decreasing level of efficiency through the communication. The performance of throughput and the convergence rate to be improved. The high throughput enables the communication with the high efficiency of transmission. The information may leads to reduce the end-to-end delay, packet delivery ratio with the less execution time. To overcome this problem, SDRNFC method to be utilized.

Stochastic Discriminant Random Forest Node Classifier – The challenge may arise for a time-to-event response subjected to the mean time of the communication. To estimates the individual classification of the designed specific classification paths. The characteristics are personalized and the road information provides the conventional approaches with the less execution time.

Trust Aware extreme Gradient Boosting Node Classification based Secured Routing - In this method provides the cyber threats and attacks to be detected. The machine learning approach based classification algorithm that provides the significant differences among the classifiers. The classified communication to be developed and the throughput lesser than the due to the communication.

6. CONCLUSION

In an urban setting, routing in VANETs is a challenging task. The increased mobility of the nodes will cause routing problems. Therefore, the reasons for the service's declining quality will make it a difficult problem. Stochastic Discriminant Random Forest Node Classifier and TAXGBNC-SR with the usage of the weighted end to end delay technique will be used to replace this problem. Here, the quickest, safest path was found using this technique. The simulation results ultimately demonstrated that the stochastic discriminant random forest node classifier can produce improved packet delivery ratio, latency, throughput, and execution time that outperforms well, demonstrating the method's effectiveness.

REFERENCES

[1]. Tomar, R. S., Sharma, M. S. P., Jha, S., & Chaurasia, B. K. (2019). Performance Analysis of Hidden Terminal Problem in VANET for Safe Transportation System. In Harmony Search and Nature Inspired Optimization Algorithms (pp. 1199-1208). Springer, Singapore.

[2]. Loganathan, G. B. (2019). Vanet Based Secured Accident Prevention System. International Journal of Mechanical Engineering and Technology, 10(6).

[3]. Karimzadeh Motallebiazar, M., Mariano de Souza, A., Zhao, Z., Braun, T., Villas, L., Sargento, S., & Loureiro, A. A. (2019). Intelligent Safety Message Dissemination with Vehicle Trajectory Density Predictions in VANETs.

[4]. Koti, R. B., & Kakkasageri, M. S. (2019, March). Intelligent Safety Information Dissemination Scheme for V2V Communication in VANETs. In 2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN) (pp. 1-6). IEEE.

[5]. Jose, A. A., Pramod, A., Philip, G., & George, S. J. (2019). sybil attack detection in vanet using spider-monkey technique and ecc. International Journal, 8(3).

[6]. Nguyen, V., Khanh, T. T., Oo, T. Z., Tran, N. H., Huh, E. N., & Hong, C. S. (2019). A Cooperative and Reliable RSU-Assisted IEEE 802.11 P-Based Multi-Channel MAC Protocol for VANETs. IEEE Access, 7, 107576-107590.

[7]. Tomar, R. S., Sharma, M. S. P., Jha, S., & Sharma, B. (2019). Vehicles Connectivity-Based Communication Systems for Road Transportation Safety. In Soft Computing: Theories and Applications (pp. 483-492). Springer, Singapore.

[8]. Li, W., Song, W., Lu, Q., & Yue, C. (2019). Reliable Congestion Control Mechanism for Safety Applications in Urban VANETs. Ad Hoc Networks, 102033.

[9]. Naja, A., Boulmalf, M., & Essaaidi, M. (2019). Toward a New Broadcasting Protocol to Disseminate Safety Messages in VANET. In Recent Advances in Electrical and Information Technologies for Sustainable Development (pp. 161-170). Springer, Cham.

[10]. Benkirane, S. (2019, April). Road Safety Against Sybil Attacks Based on RSU Collaboration in VANET Environment. In International Conference on Mobile, Secure, and Programmable Networking (pp. 163-172). Springer, Cham.

[11]. Cui, J., Wu, D., Zhang, J., Xu, Y., & Zhong, H. (2019). An Efficient Authentication Scheme Based on Semi-Trusted Authority in VANETs. IEEE Transactions on Vehicular Technology, 68(3), 2972-2986.

[12]. Ramakrishnan, B., Sreedivya, S. R., & Selvi, M. (2015). Adaptive routing protocol based on cuckoo search algorithm (ARP-CS) for secured vehicul ar ad hoc network (VANET). International Journal of computer networks and applications (IJCNA), 2(4), 173-178.

[13]. Erskine, S. K., & 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), 776

[14]. Limbasiya, T., & Das, D. (2019). ESCBV: energy-efficient and secure communication using batch verification scheme for vehicle users. Wireless Networks, 25(7), 4403-4414.

[15]. Subasi, A., Jukic, S., & Kevric, J. (2019). Comparison of EMD, DWT and WPD for the localization of epileptogenic foci using Random Forest classifier. *Measurement*, *146*, 846-855.

[16]. Jaballah, W. B., M. Conti and C. Lal (2020). "Security and Design Requirements for Software-Defined VANETs." Computer Networks: 107099.

[17]. Mazilu, S., M. Teler and C. Dobre (2011). Securing vehicular networks based on data-trust computation. 2011 International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, IEEE.

[18]. SathyaNarayanan, P. (2019). "A sensor enabled secure vehicular communication for emergency message dissemination using cloud services." Digital Signal Processing **85**: 10-16.

[19]. Yiliang, H., L. Xi, J. Di and F. Dingyi (2017). Attribute-based authenticated protocol for secure communication of VANET. 2017 29th Chinese Control And Decision Conference (CCDC), IEEE.