An Intelligent Transport System in VANET using Proxima Analysis

Satyanarayana Raju K[1], Dr. Selvakumar K[2]
Department of Information Technology, Annamalai University, Chidhambaram, India

***Abstract*—There is no proper structure for Vehicular ad hoc networks (VANETs). VANET generates several mobility vehicles that move in different directions by connecting the vehicles and transferring the data between the source and destination which is very useful information. In this system, a small network is created with vehicles and other devices that behave like nodes in the network. Sometimes for better communication, VANET uses suitable hardware for improving the performance of the network. Reliability is one of the significant tasks that perform the needful operations and methods based on the conditions at a specific time. To disturb the VANETS, the attacker tries to hit the server and that causes damage to the server. This paper mainly focused on detecting the falsification nodes by analyzing the behavior of the models. In this paper, an improved intelligent transportation system (ITS) Proxima analysis is introduced to find the accurate falsification nodes. The proposed approach is the integration of KNN and RF with Proxima analysis. The main aim of the Proxima is to analyze the falsification nodes within the network and improve the mobility of the vehicles by sending source to destination without any miscommunication.**

***Keywords*—Vehicular Ad hoc Network (VANET); intelligent transportation system (ITS); KNN; RF**

I. Introduction

VANETs is a very fast-growing field in wireless technology. VANET is considered as a sub-class of MANET in which the moving vehicles are considered as nodes or routers which are used to exchange the messages between the vehicles or access points. All the vehicles in this network are connected within the range of 100 to 900 meters by using 802.11p. This network will support both vehicles to a vehicle (V2V) and vehicle to infrastructure (V2I) for better communication within the network. The proposed approach ITS is used to increase road safety and provides a better travel experience for driver and passengers [1], [2].

Generally, VANET can increase traffic safety and effectiveness. Before starting the VANET network, privacy and security are two issues that are addressed before starting the network and data transmission [3]. In security, authentication is one of the significant tasks to provide privacy for the nodes present in the VANET network. With anonymous authentication, the network has to face challenges in verifying the vehicles in the network. This leads to a loss of data and communication between the vehicles [4]. This also fails to verify the huge data per second in VANETs. In VANETs, several advantages for routing protocols are identified based on the nature of the vehicle movements. A lot of research has been done on the issues of routing protocols such as scalability and reliability around the urban VANETs [5]. Nowadays Intelligent transportation systems (ITSs) are becoming more popular for connecting vehicles very efficiently and with better coordination. ITS's is the internal part of the VANET. This technique is mainly used to transfer the data between the nodes to improve security, efficiency, and reliability. VANETs are the sub-domain in the mobile ad-hoc networks (MANETs) and these are the integral parts of the ITSs. Strongly interconnected vehicles are used to sense the data and transfer the data based on location, traffic, environment, and urgent services [6].

VANET is showing attention because of several significant applications that are related to road safety and control of traffic. VANET mainly focused on improving road safety and controlling traffic. In smart cities, a lot of problems occur due to the heavy traffic due to the falsification nodes or vehicles. Falsification nodes create a lot of network damage that will lose the data which is transferred by the vehicles. By detecting the falsification nodes the Intelligent Transportation System (ITS) will improve the routing in the network. Based on the behavior of the vehicles falsifications vehicles are detected.

Fig. 1 shows the sample vehicles in the VANET's by using the SUMO simulator. All the yellow vehicles are normal vehicles that are having mobility. Fig. 2 shows the process of visualizing the VANET network by applying the proposed approach and its functionalities.

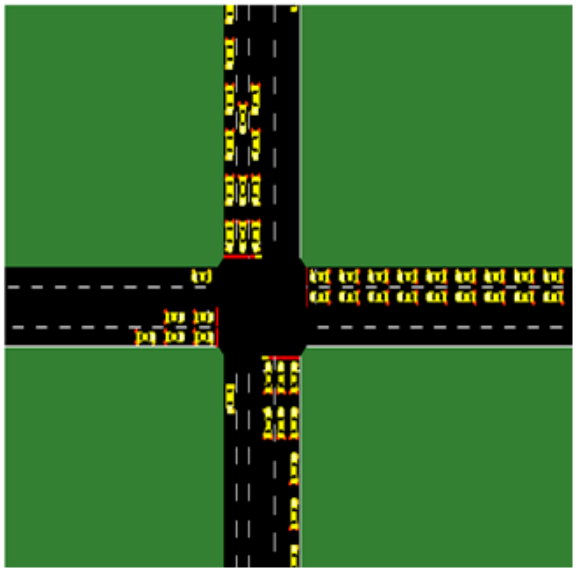

Fig. 1. Shows the Mobility of the Vehicles according to the Signals.

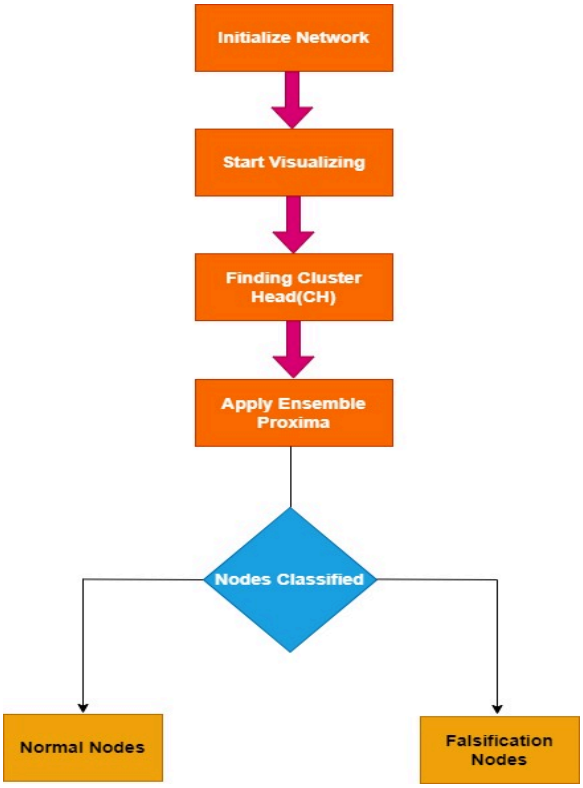

Fig. 2. Steps for Processing of Improved Intelligent Transportation System (ITS) Proxima Analysis.

II. Literature Survey

Over the last few years, Intelligent Transportation Systems (ITS) is showing an improvement in the movements of vehicles on the roads. The aim of the ITS is to provide better and more comfortable driving for the VANET vehicles that are present in the network by updating the information about the roads. Over the past many years, many researchers developed several approaches that are discussed in this section.

A. Ullah et al., [7] presented the location-based routing (LBR) protocol which is used to present the taxonomy. This approach is focused on analyzing the parked vehicles that are nearer to the junction for the selection of the path. This approach supports only less packet delivery, delay, and data transmission time and is more expensive. Abu Talib et al., [8] presented various security issues and solutions for the various issues and challenges in VANETs. This article also discussed the various types of attacks and various solutions that are implemented by solving several threats and shows the performance.

Abdul Quyoom et al., [9] proposed the ITS which is integrated with multifunctional system that collects a huge amount of data from several resources: Vision-Driven ITS (the sample data is collected from various visual sensors and utilized the vehicle and pedestrian detection); Multisource-Driven ITS (inductive, laser and GPS detectors); Learning-Driven ITS (this will reduce the collisions between the vehicles); and Visual-Driven ITS (this is used to find the abnormal traffic patterns and take required measures).

J. Cui et al., [10] introduced the adaptive approach that controls the traffic based on the communication among the cars. This system reduces the waiting time of the vehicles that are interacted with the decrease in queue length. To increase this system, clustering is adopted by utilizing the intersection of vehicles. By using this approach, the density of vehicles that are present in the cluster is calculated by using the clustering approach. The DBCV approach is used to increase the accuracy of the results. This approach is a combination of cluster and strategic diffusion methods which is utilized and collects the density information. Based on the movement and directions the clusters are formed within the region. By using the GPS and maps the direction of the vehicles is measured.

Saif Al-Sultan et al. [11] control the systems that are based on the other vehicles' data. Every vehicle is designed with a short communication device that controls the nodes that are combined with traffic lights. The node that controls this system plays the adaptive signal system. VANETs characteristics makes security and trust management as challenging issues. Different types of security threats and attacks persist in VANET [12].

III. Several Types of Attacks that Occur at the Simulation Time

Denial of Service (DoS) is an attack that can occur in the network [13]. There are two types of attackers, inside attacker and outside attacker. An inside attacker can jam the network by transmitting fake messages and stopping the network connections. The outside attacker continuously circulates the fake messages with fake signatures that use the bandwidth or other resources of a targeted vehicle. With this attack, VANET loses the ability to give services to the actual vehicles [14]. The main aim of this attack is to send the fake message to TSU and also to the actual vehicle to create a jam in the network.

The malicious nodes in the black hole attack [15], try to have the best route for the destination node and show that the data should transfer from this route by transferring the fake route information. A malicious node in this attack mainly drops or misuses the stopped packets without sending them to anyone [16]. This attack mainly creates the black hole area that creates the number of malicious vehicles and they are not interested to receive the messages from the actual vehicles [17].

Malicious vehicles in Wormhole attack [18], received the data at one point and replay it with another malicious vehicle by utilizing a wormhole high-speed link (tunnel) and data transfer from source to destination continuous by using malicious vehicles. This attack shows the huge impact on preventing finding the valid routes & menaces the security by transferring data packets. In this attack, the tunnel is used to broadcast the secret information by using two malicious vehicles.

The malicious vehicles in the sinkhole attack telecast the dummy routing information within the network [19]. This can easily attract the network traffic towards routing. This attack shows the huge impact on the network that complicates and reduces the performance by changing the data packets or

dropping the packets [20]. The malicious vehicles in this network drop the data packets that are received from the authorized vehicle & telecast the fake routing info to the authorized vehicles on backside [21].

The malicious vehicles in the Sybil attack create a huge number of fake signatures that take overall control of VANET and insert the fake data in the network to threaten the legal vehicles. This attack will create the illusion among the multiple vehicles that creates a huge impact on the VANET network. This attack shows the huge impact on the network because of spoofing the signatures or places of other vehicles in the vehicular network [22]. This attack aims to create the fake identities of multiple vehicles and generates huge vehicles on the network [23].

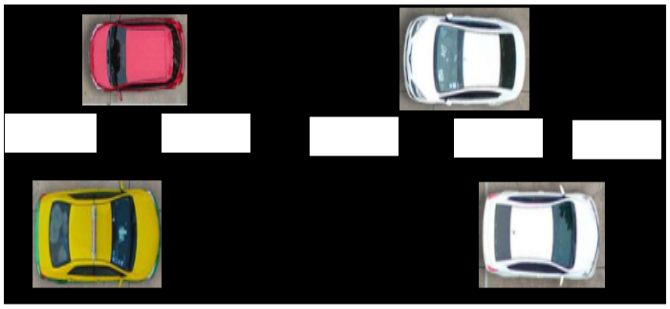

Fig. 3. In this Network Red Color Vehicle is considered as Malicious Node and other Vehicles are Normal Vehicles.

A. Random Forest (RF) for Detecting the Falsification Nodes

Random Forest (RF) is one of the hybrid approaches that follows the rule of bagging. It is an ensemble approach. Fig. 3 shows the normal nodes and malicious nodes by representing the malicious node with red color and normal vehicles are represented with white and yellow. This approach is a continuation of the decision tree (DT). DT is used to develop the information gain technique represented in Equation 1 and Equation 2.

To calculate the entropy value at every vehicle the equation (1) is given below:

$$E(s) = \sum p_i \log_2 p_i \quad (1)$$

After entropy is calculated, the information gain is measured at every attribute to get the better decision for the vehicles.

$$\text{Gain}(S, A) = \text{Entropy}(S) - \frac{\Sigma_{v \in \text{values}(A)} |S_v|}{|S| \text{Entropy}} (S_v) \quad (2)$$

Based on the entropy value the vehicles are classified according to the behavior.

The output of the random forest is given as an input to the KNN approach for filtering the falsification nodes according to the distance measure.

B. Applying KNN for RF Output Vehicles

KNN is one of the significant approaches used to classify the complex dataset. This is one of the better approaches for detecting the falsification nodes. Better training is given to the system for effective output. This approach analyzes the behavior of the vehicles in the real-time network. Based on the distance and direction the training generates better properties from the nodes. From the moving vehicles, the test runs are measured when the vehicles are in the same direction, different directions, and the location of vehicles are collected. For training, the dataset is utilized for the KNN model. If any abnormal behavior is identified among the vehicles, the distance and directions are identified as an input to the KNN classifier. The outputs of the KNN are represented as 0 or 1. 0 indicates the dangerous node and 1 indicates the safe. The KNN Algorithm Pseudocode:

1. Training and testing data is loaded
2. K-value is selected.
3. Every point in test data:
   - Euclidean distance is used for training data points such as (a, b) and (-a, -b).

$$d = \sqrt[2]{(a\text{^}2 + b\text{^}2} \quad (3)$$

   - List of Euclidean distances are stored and sorted.
   - First k points are chosen.
   - Based on the majority the class is assigned.

4. End

Above algorithm represents, K=5 i.e. five nearest neighbors are compared for every instance that requires to be classified. Hence it is known that the nearest vehicles are considered as normal vehicles and other vehicles are falsification vehicles based on the distance.

C. Measuring the Falsification Vehicles in the VANETs

In this paper, the proposed approach mainly focused on measuring the optimized routing by using proxima analysis. This approach considered the output of the KNN for proxima analysis. Proxima analysis is mainly focused on measuring the distance among the vehicles in the network. In this scenario, a proximity sensor plays the major role in detecting the distance among the vehicles and analyses the movement of vehicles. Here, the clustering head plays the major role to detect the abnormal vehicle.

- If the vehicle is having abnormal behavior then the vehicle drops or fakes the data packets received to create congestion in the network and mislead the vehicles and damage the malicious messages for their purpose.
- Truthful nodes forward the correct messages to the several nodes in the network and create the accurate messages for transmission.
- The main aim of this system is to monitor the behavior of the network. The monitoring process of the vehicles is called as “verifier” vehicles. Verifier is smaller or equal to Td compared with the Td of vehicle V, and this is placed inside the region z (V, Cluster Head (CH)). The intersection region is created for both vehicles named as V and CH.

By using these steps, the verifiers are monitored with V are send reports to CH [24]. The CH is equal to its transmission range and the V is obtained from the region and it is represented with Equation (4).

$$\text{Area (V)} = \text{TR(V)} - T_f(S_{max} - S_{min}) \quad (4)$$

Where,

S_{max} - Legal maximum speed of the vehicle. S_{min} - Legal minimum speed of the vehicle.

T_f – Packet Latency.

CH – Cluster Head.

Thus this will improve the routing of the vehicles by using proxima analysis.

Algorithm Steps for Proxima Analysis

Input: Nodes in the network Vehicles)

Output: Malicious Nodes (Vehicles)

Initialize variables N-Network, n-nodes or vehicles, r-region.

Step 1: N_{mob}-telecast the messages from all the vehicles.

Step 2: if ($N_{mob} \geq 2$)

Step 3: the mobility started it indicates presence of multiple nodes //Explains the status of the mobility

Else

Mobility not started.

Step 4: Calculate Euclidean distance by using Equation (3)

Step 5: arraylist [nearest nodes N_n] //Store the nearest nodes in arraylist.

Step 6: By using the given function nd_malv(Packet *p) the malicious vehicle is detected based on behavior.

```
if(mal==true)
{
drop(p,DROP_RTR_ROUTE_LOOP);
}
```

By showing the packet dropping rate the malicious nodes are identified.

Step 7: Malicious nodes are detected.

Table I shows the malicious and normal nodes. It is observed that in the existing approach there are missing nodes that are not considered by the existing approach. Compare with existing system approach the proposed approach detect very less missed vehicles.

TABLE I. SHOWING THE MALICIOUS AND NORMAL NODES

Total No of Nodes	Malicious Nodes		Normal Nodes	
	ES	PS	ES	PS
50	13	23	28	35
100	26	36	45	59
150	38	99	48	99
200	37	138	53	144

IV. PERFORMANCE METRICS

A. Area under ROC Curve (AUC)

The overall proportion of true positives (malicious nodes accurately classified as malicious) compare with the proportion of false positives (not malicious and it is wrongly classified as malicious).

This is one of the efficient approaches that measures the following equation, Where t = (1 – specificity) and ROC (t) is sensitivity.

$$\text{AUC} = \int_0^1 \text{ROC(t)dt} \quad (5)$$

B. Accuracy

In machine learning, this is one of the significant metric that shows the overall accuracy of the data transmission and the performance of proposed approach. The overall accuracy is calculated by using below equation:

$$\text{Accuracy} = \frac{\text{TN+TP}}{\text{TP+TN+FP+FN}} \quad (6)$$

C. Precision

Precision is one of the significant factors in analyzing the results. High precision represents the low false positive rate.

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \quad (7)$$

D. Recall or Sensitivity

Recall is also one of the parameter to analyze the results. High recall relates to a low false negative rate.

$$\text{Recall} = \frac{\text{TP}}{\text{TP+FN}} \quad (8)$$

E. Specificity

This measures the overall proportion of original negatives (Falsification Nodes), where the results are predicted as negative.

$$\text{Specificity} = \frac{\text{TN}}{\text{TN+FP}} \quad (9)$$

F. F1-Score

This is one of the measures that scores the weighted average of Precision and Recall. This will consider the false positives and negatives from the account. This will also show the uneven distributed classes.

$$\text{F1} - \text{Score} = \frac{2*(\text{Precision}*\text{Recall})}{(\text{Precision+Recall})} \quad (10)$$

Results and graphs were obtained with the following parametric values shown in Table II.

TABLE II. PARAMETRIC ENVIRONMENT

Metric	**Values**
Total No of Nodes	50-200 Nodes
Average Node Speed	50 m/s
Simulation Time	90-100 Sec

Table III and Fig. 4 show the performance of existing approaches by showing the AUC curve performance for 50, 100, 150 and 200 nodes. Among this the proposed approach Ensemble Proxima achieved the better results.

TABLE III. PERFORMANCE OF MACHINE LEARNING (ML) ALGORITHMS SHOWING AUROC

Total No of Nodes	KNN	KNN_RF	Ensemble Proxima
50	0.73	0.78	0.89
100	0.74	0.76	0.91
150	0.75	0.76	0.91
200	0.75	0.76	0.92

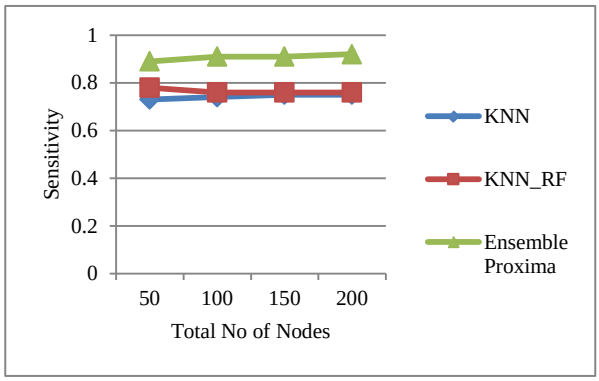

Fig. 4. Showing ROC for all the ML Algorithms.

Table IV, Fig. 5 and Fig. 6 show the performance of existing approaches by showing the Accuracy performance for 50, 100, 150 and 200 nodes. Among this the proposed approach Ensemble Proxima achieved the better results.

TABLE IV. PERFORMANCE OF MACHINE LEARNING (ML) ALGORITHMS SHOWING ACCURACY

Total No of Nodes	KNN	KNN_RF	Ensemble Proxima
50	84.49	89.85	93.03
100	85.12	88.89	94.12
150	86.45	89.89	95.12
200	85.56	88.98	95.78

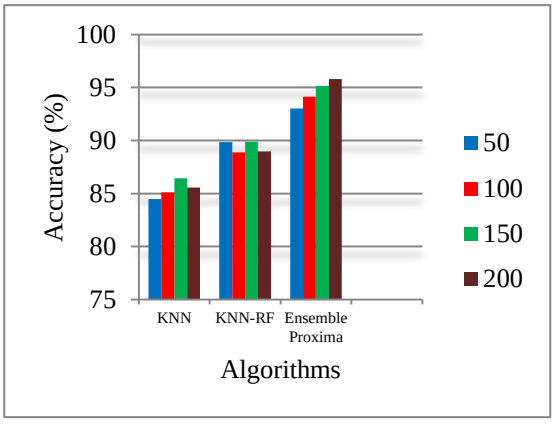

Fig. 5. Performance of Machine Learning (ML) Algorithms showing Accuracy.

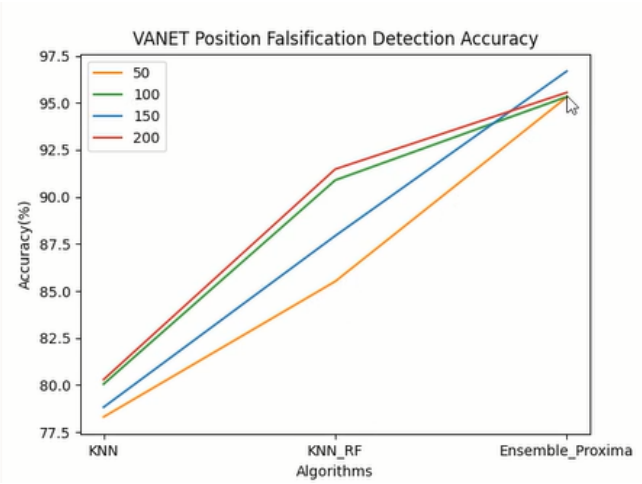

Fig. 6. Shows the Line Graphs based on Performance of Algorithms.

Table V, Fig. 7 and Fig. 8 explained about the performance of Existing and Proposed Algorithms. The performance is showing for precision parameter.

TABLE V. PERFORMANCE OF MACHINE LEARNING (ML) ALGORITHMS SHOWING PRECISION

Total No of Nodes	KNN	KNN_RF	Ensemble Proxima
50	83.79	88.15	94.63
100	84.32	87.89	95.42
150	85.15	88.89	96.32
200	84.16	89.98	96.78

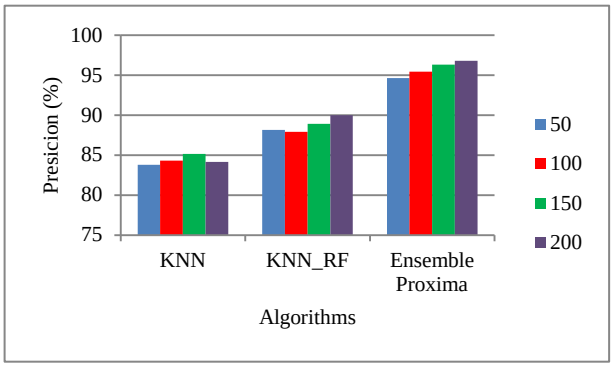

Fig. 7. Shows the Comparative Analysis of Existing and Proposed Algorithms for Precision.

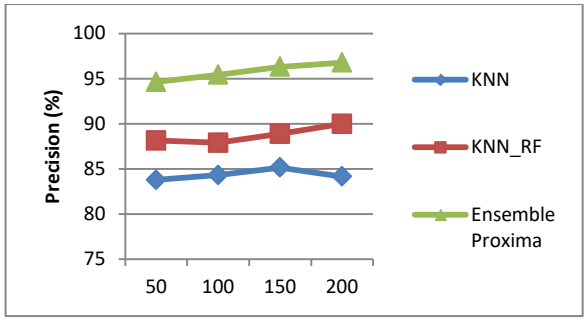

Fig. 8. Shows the Comparative Analysis of Existing and Proposed Algorithms for Precision using the Line Graphs.

Table VI, Fig. 9 and Fig. 10 show the performance comparison among the existing and proposed ML algorithms by showing the Recall. The performance is represented by showing bar graphs and line graphs.

TABLE VI. PERFORMANCES OF MACHINE LEARNING (ML) ALGORITHMS SHOWING RECALL

Total No of Nodes	KNN	KNN_RF	Ensemble Proxima
50	83.19	88.45	94.99
100	85.12	89.89	95.77
150	86.45	89.89	96.12
200	84.56	87.98	96.78

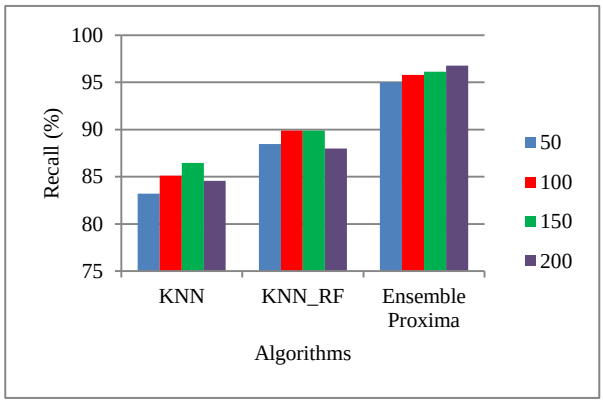

Fig. 9. Shows the Comparative Analysis of Existing and Proposed Algorithms for Recall.

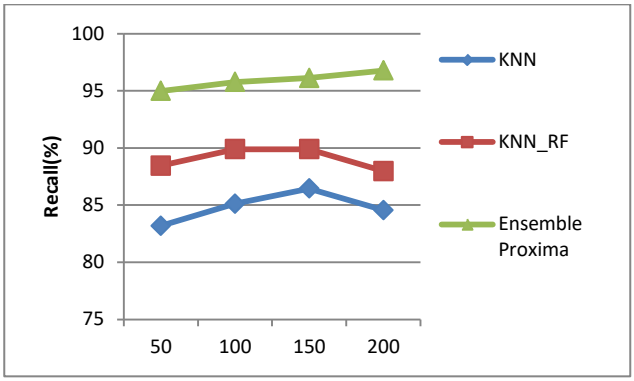

Fig. 10. Shows the Comparative Analysis of Existing and Proposed Algorithms for Recall using the Line Graph.

Table VII, Fig. 11 and Fig. 12 show the performance comparison among the existing and proposed ML algorithms by showing the F1-Score. The performance is represented by showing bar graphs and line graphs.

TABLE VII. PERFORMANCE OF MACHINE LEARNING (ML) ALGORITHMS SHOWING F1-SCORE

Total No of Nodes	KNN	KNN_RF	Ensemble Proxima
50	83.23	89.85	93.43
100	84.55	88.81	94.53
150	85.67	88.37	96.42
200	86.78	87.34	96.82

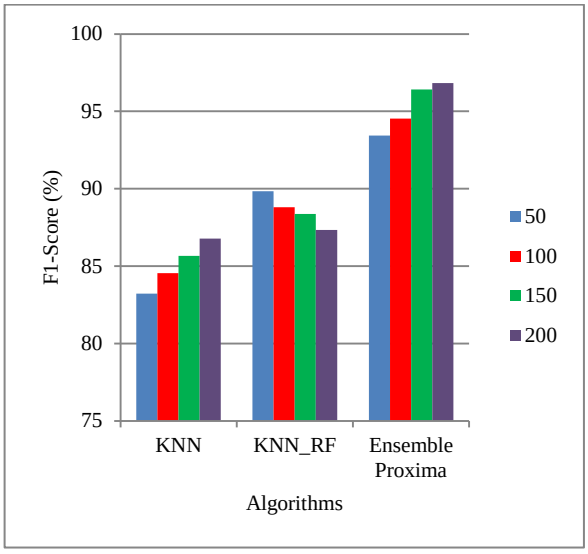

Fig. 11. Shows the Comparative Analysis of Existing and Proposed Algorithms for F1-Score.

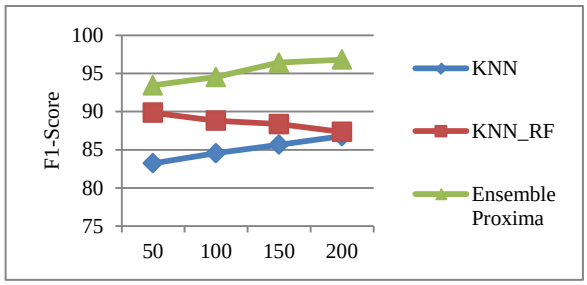

Fig. 12. Shows the Comparative Analysis of Existing and Proposed Algorithms for F1-Score using the Line Graph.

V. CONCLUSION

In this paper, the proposed approach focused on finding the falsification vehicles by using integrated Proxima analysis. The proposed approach is the combination of RF and KNN that helps to detect the falsification nodes based on the behavior of the vehicles. Falsification vehicles attack the network and cause breaking traffic rules such as over-speeding and wrong-way driving. It also provides a GUI which can be used by the traffic department to monitor roads and send help in case of an accident. The proposed method was cautiously evaluated in a traffic simulation environment, SUMO. The performance of the proposed approach has improved the performance in terms of the accuracy of AUROC. In future, an improved learning approach is combined with the various heuristic approaches to get the better detection of malicious nodes.

REFERENCES

[1] Javed Muhammad Noman et al., "VANET's Security Concerns and Solutions: A Systematic Literature Review," in Proceedings of the 3-rd International Conference on Future Networks and Distributed Systems (ICFNDS) ACM, pp. 1- 12, July 1-2, 2019.

[2] Abdul Quyoom, "Security Issues of Vehicular Ad Hoc Networks in OSI layers," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, ISSN: 2456-3307, vol. 2, no. 4, 2017.

[3] D. He, S. Zeadally, B. Xu and X. Huang, "An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular

Ad Hoc Networks," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 12, pp. 2681-2691, Dec. 2015, doi: 10.1109/TIFS.2015.2473820.

[4] M. Azees, P. Vijayakumar and L. J. Deboarh, "EAAP: Efficient Anonymous Authentication With Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks," in IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 9, pp. 2467-2476, Sept. 2017, doi: 10.1109/TITS.2016.2634623.

[5] C. Cooper, D. Franklin, M. Ros, F. Safaei and M. Abolhasan, "A Comparative Survey of VANET Clustering Techniques," in IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 657-681, Firstquarter 2017, doi: 10.1109/COMST.2016.2611524.

[6] T. Chatterjee, R. Karmakar, G. Kaddoum, S. Chattopadhyay and S. Chakraborty, "A Survey of VANET/V2X Routing From the Perspective of Non-Learning- and Learning-Based Approaches," in IEEE Access, vol. 10, pp. 23022-23050, 2022, doi: 10.1109/ACCESS.2022.3152767.

[7] A. Ullah, X. Yao, S. Shaheen and H. Ning, "Advances in Position Based Routing Towards ITS Enabled FoG-Oriented VANET–A Survey," in IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 2, pp. 828-840, Feb. 2020, doi: 10.1109/TITS.2019.2893067.

[8] Abu Talib, Manar, et al., "Systematic literature review on Internet-of-Vehicles communication security," International Journal of Distributed Sensor Networks, ISSN: 1550147718815054, vol. 14, no. 12, 2018.

[9] Abdul Quyoom, MohdSaleem, MudasserNazar, Yusera Farooq Khan, "VANETs Applications, Challenges and Possible Attacks: A Survey, "International Journal of Advanced Research in Computer and Communication Engineering, ISO 3297:2007 Certified Vol. 6, Issue 7, July 2017.

[10] J. Cui, L. Wei, J. Zhang, Y. Xu, and H. Zhong, "An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks," IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 5, pp. 1621-1632, 2019. https://doi.org/10.1109/TITS.2018.2827460.

[11] Saif Al-Sultan, Moath M. Al-Doori, Ali H. Al-Bayatti, and HussienZedan, "A comprehensive survey on vehicular ad hoc network," Journal of Network and Computer Applications, vol.37, no. 1, pp. 380-392, 75 80 85 90 95 100 F1-Score (%) Algorithms 50 100 150 200 2014. https://doi.org/10.1016/j.jnca.2013.02.036.

[12] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy, "IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 2, pp. 760-776, 2019. https://doi.org/10.1109/TITS.2018.2818888.

[13] Abdul Quyoom, Raja Ali and Devki Nandan Gouttam, "A Novel Mechanism of Detection of Denial of Service Attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA)," in Proceedings of the IEEE International Conference on Computing, Communication and Automation (ICCCA2015), pp. 414- 419, 2015.

[14] Jafer, Muhammad, et al., "Secure Communication in VANET Broadcasting," ICST Transaction on Security Safety, vol.5, no.17, 2019.

[15] Karimireddy, T. and Bakshi, A., "A Hybrid Security Framework for the Vehicular Communications in VANET," in Proceedings of the International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 1929-1934, 2016.

[16] Satyanarayana Raju K, Dr. Selvakumar K, “Dynamic and Optimized Routing Approach (DORA) in Vehicular Ad hoc Networks (VANETs)”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 13, ISSUE No. 3, 2022. https://thesai.org/Publications/ViewPaper?Volume=13&Issue=3&Code=IJACSA&SerialNo=20

[17] Md Whaiduz-zaman, Mehdi Sookhak, Abdullah Gani, and Rajkumar Buyya, "A survey on vehicular cloud computing," Journal of Network and Computer Applications, vol. 40, pp. 325-344, 2014. https://doi.org/10.1016/j.jnca.2013.08.004.

[18] Sumra, Irshad Ahmed, Iftikhar Ahmad, HalabiHasbullah, and J-L. bin Ab Manan, "Classes of Attacks in VANET," in Proceedings of Saudi International Electronics, Communications and Photonics Conference (SIECPC), pp. 1-5, 2011.

[19] A. Festag. "Cooperative intelligent transport systems standards in Europe," Communications Magazine, IEEE, vol. 52, no.12, pp. 166-172, Dec. 2014. https://doi.org/10.1109/MCOM.2014.69799 70.

[20] Hussain Rasheed, Fatima Hussain, and Sherali Zeadally, "Integration of VANET and 5G Security: A review of design and implementation issues," Journal of Future Generation Computer Systems, pp. 843-864, 2019.

[21] Kumar Mr Kamal, and Rahul Malhotra, "Analysis of Sybil Attack Isolation Technique in VANET," International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 8, no. 5, pp.187- 192, May 2019.

[22] Singh Avinash et al., "Implementing Security Services in VANET Using Cryptography Based on Artificial Neural Network," Journal of Computer and Mathematical Sciences, vol. 10, no. 9, pp. 1573-1584, 2019.

[23] Karagiannis D. and Argyriou A., "Jamming attack detection in a pair of RF communicating vehicles using unsupervised machine learning," Vehicular Communications, vol.13, pp. 56-63, 2018. https://doi.org/10.1016/j.vehcom.2018.05.00 1.

[24] Safi, Q.G.K., Luo, S., Wei, C., Pan, L. and Yan, G., "Cloud-based security and privacy-aware information dissemination over ubiquitous VANETs," Computer Standards and Interfaces, vol.56, pp. 107- 115, 2018. https://doi.org/10.1016/j.csi.2017.09.009.