**An enhanced VANET paradigm for reliable communication based on LoRa technology.**

**Abstract**

The vehicular ad-hoc networks (VANET) are being developed to enable effective vehicle communication and the exchange of traffic information. However, the VANET is also vulnerable to various security threats, including Denial-of-Service (DoS) attacks. By identifying system attacks, it is imperative to provide more trustworthy and secure communication amongst all the vehicles that are a part of the VANET system. In this research, a novel enhanced VANET paradigm is proposed for secure and reliable communication based on LoRa (Long Range) technology. In this research, the DoS attack was initially detected using data on the implicated automobiles using an upgraded fuzzy method known as Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS). Then the seagull optimization is used to enhance the capacity of the nodes. An improved Deep Deterministic Policy Gradient (DDPG) algorithm is used to find the optimal path. The developed model is then contrasted with other traditional methods in the second step to determine its superiority. Finally, the obtained results show that at node 60, the value of delay, energy consumption, and drop, is 13.8547, 1.874, and 0.1214 respectively which is better than any other existing techniques.

**Keywords:** VANET, LoRa technology, TOPSIS, Seagull optimization, Deep Deterministic Policy Gradient.

1. **Introduction**

In the last few years, a type of technology called VANETs has grown into an important area of study. VANET is a form of network that is produced by the notion of constructing a network of automobiles to cater to a particular need or circumstance [1]. As an ad-hoc network, it is a kind. Despite its many advantages, VANET nevertheless presents a significant number of difficulties, including the provision of quality service, high connection, and bandwidth, and the of network that is established using this concept. The usage of reliable networks called VANETs by cars for communication while traveling on roads or in urban areas has now been developed protection of individual privacy and the safety of vehicles [2].

The primary purpose of VANET is to facilitate the establishment and maintenance of a communication network between a collection of vehicles that do not rely on a centralized base station or operator of any kind. One of the most important uses of VANET is in emergency medical situations, such as when there isn't an infrastructure, but it is essential to transmit information to save human lives [3]. Since VANET has so little in the way of infrastructure, more tasks fall on the vehicles. Every vehicle is added to the network and takes on the responsibility of managing and controlling the communication on that network in addition to fulfilling its own communication needs [4].

The use of VANET technology has several potential benefits, including a decrease in the number of automobile collisions as well as an improvement in the overall quality of the driving and traveling experience through the streamlining of various payment procedures, such as those for tolls, parking, and fuel, among other things. Users of roads use a variety of applications for a variety of purposes, including but not limited to safety and efficiency; traffic control; information and entertainment; comfort and maintenance; music sharing; and network gaming [5].

1. **Vehicular ad hoc network (VANET)**

It is anticipated that VANET enhances the driving experience by providing more safety, security, durability, and informational capabilities [6]. In most cases, a VANET includes automobiles communicating with one another via the use of a roadside device (RSU). The onboard unit (OBU), which is a part of the VANET design, is comprised of a receiver and a wireless transmitter [7]. It is made up of two principal domains, which are referred to as the Motorized Area and the commercial Domain respectively. Within the realm of automobiles, the OBU is linked to the Application Unit (AU). During the time spent in the ad-hoc mode, moving vehicles are connected to an appropriate gateway (GW) in an inter manner via RSUs. The RSU communicates with the OBU, which has an open connection to the internet, by sending a message [8].

Communication in VANET takes place between individual cars (referred to as V2V), as well as between individual vehicles and infrastructure (referred to as V2I), and also between personal cars and broadband services (V2B). The Vehicle-to-Vehicle and Vehicle-to-Remote Support Unit (V2V-RSU) Network (VANET) is used for brief transmission between moveable host automobiles and also between vehicles and RSUs Figure 1 [9]. Because of the potential of distribution centres to allocate resources towards integrated activities, the RSU has been regarded as one of the most important components of the VANET. RSUs often come with very high expenses linked to both their installation and their maintenance. Figure 2 presents a simplified representation of a VANET [10]. Similarly, academics have suggested the exploitation of parked automobiles as an expansion of RSUs to address additional difficulties such as the probability sampling of RSUs as well as high-level task stress. These vehicles are in charge of assigning work to RSUs and ensuring that other vehicles can obtain the appropriate updates.

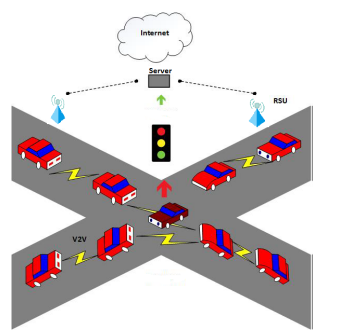


Figure 1: VANET system model [9]

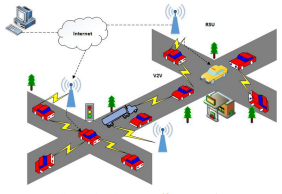


Figure 2: VANET traffic congestion.[10]

1. **LoRa technology**

LoRa is a communication technology that enables low-power, wide-area wireless communications. It can support hundreds of thousands of different devices at once. LoRa is a low-power wide area network (LPWAN) communication technology that uses the Industrial, scientific, and medical (ISM) band). Even though it has a vast network penetration of around 20 kilometers or more while employing a transmitting power of fewer than 14 decibels, it has been widely documented and is used in both academic and commercial settings. While LoRa connectivity establishes a national forum and makes it possible for users to establish autonomous low-power wireless connections while depending on the third-party architecture, these benefits are not exclusive to one another. To develop LoRa systems that are useful, there are currently several technological challenges that need to be conquered. These challenges include connection management, resource allocation, constant communications, and security. This paper provides a comprehensive introduction to LoRa networking. It discusses the technical challenges involved in establishing LoRa networks as well as the solutions that are currently available. Based on the in-depth investigation of the many available solutions, a few of the major issues that are associated with LoRa communication is highlighted [11]. Figure 3 depicts an overview of the overall architecture of the LoRa Connectivity [12].

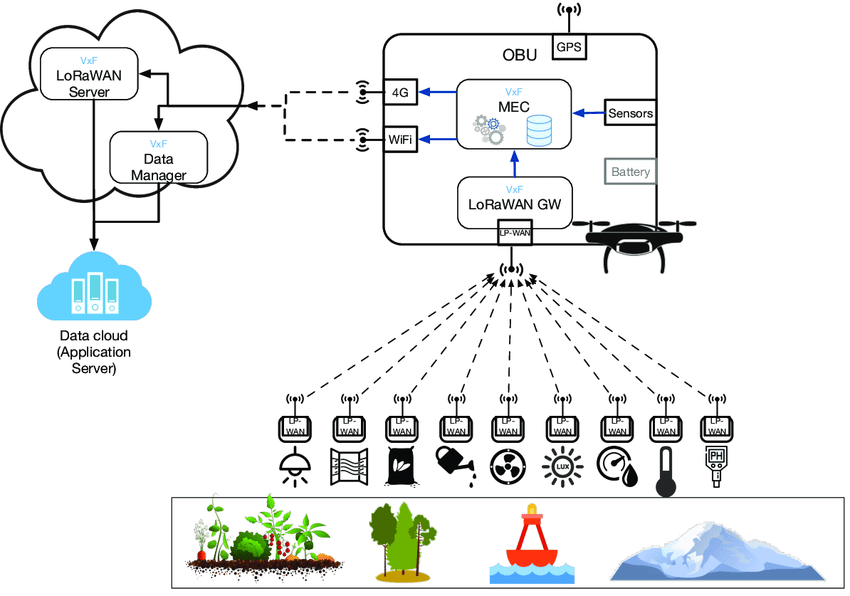


Figure 3: General architecture of the LoRa connectivity [11]

1. **Literature Of Review**

This strategy has been employed by a wide range of authors, who then presented their findings after doing a literature review:

**Valente et al., (2023) [13]** introduced the Fed Framework and constructed a testbed that links edge devices like NVIDIA Jetsons with a cloud server to create an integrated city infrastructure. Using this testbed, a lightweight federated learning (FL) framework is deployed to measure device performance, machine learning, aggregating algorithm efficacy, edge-to-server communication, and resource consumption. Using actual data gathered from the Aveiro Technology City Living Laboratory infrastructures in the city of Aveiro, conduct the assessment for the situation in which predicted vehicle mobility within and outside the city.

**Paredes et al., (2023) [14]** presented a special form of both LoRa and Flying Ad-Hoc Networks (FANETs) and conducted a systematic literature assessment based on a categorization of the communication, mobility, and energy concerns inherent in a FANET's implementation. Challenges related to the implementation of FANETs using LoRa are also highlighted, as are outstanding difficulties in protocol design.

**Naeimipoor et al., (2022) [15]** suggested a new robust and reliable multi-hop cluster-based routing system that gives priority to signals from emergency vehicles. In the suggested approach, a cluster (CH) is chosen based on the number of neighbors, the range between both the vehicle and the BS, and the S/N energy absorbed by the BS. Directly or through qualified neighboring CHs, it is the responsibility of each CH to relay data from those other member nodes to the infrastructure. To create effective resource utilization in RSU computer nodes and reduce transmission latency, the solution makes use of an epigenomic workflow technique.

**Jeong et al., (2021) [16]** proposed autonomous transportation for safe and efficient driving, with an emphasis on safety and security regarding systems, protocols, apps, and autonomous cars. For this kind of "smart" transportation to function, it is necessary to keep a close eye on road conditions and pinpoint potential dangers, and for cars to communicate with one another wirelessly to exchange sensory data that might help them avoid potentially hazardous circumstances or areas. To this end, the IEEE's Wireless Access in Vehicular Environments (WAVE) standards for then-current wireless communications (DSRC) have been finalized, and GPS-based navigation systems and smartphone apps are already quite commonplace.

**Soares et al., (2021) [17]** showed how a stochastic Petri net (SPN) model can be used to figure out how well a cooperative smart traffic light works. The average response time, resource consumption, and several abandoned requests are all quantifiable under the suggested approach. There are three examples given to show how the concept can be used in practice. Moreover, the use of microcontrollers (Raspberry Pi) to simulate traffic signals and perform actual tests to verify the suggested concept. High adaptability is achieved via the model's 18 calibratable parameters, which is adjusted by programmers and system administrators.

**Al-Khater et al., (2020) [18]** presented a primer covering a range of VANET-related topics. In this article, the field of vehicular communication and the many research obstacles that have been uncovered so far. More specifically, this article surveyed the state of the art in VANET design, transmission modeling, mathematical signal modeling considerations, routing protocols, and safety measures. This article reports the results of a comparison study of existing routing methods for VANETs. The most significant problems with routing algorithms were also brought to light.

**Fourati et al., (2020) [19]** suggested the use of a vehicle-centric, interest-based clustering peer-to-peer network (ICN) clustering mechanism. ORK IN RELATION: latest works (published in 2018–2020) on state-of-the-art clustering methods Different clustering algorithms employ different criteria (such as speed, number of neighbors, trust degree, location, and acceleration) in selecting CHs, and the resulting number of CHs might vary widely. By combining a clustering approach with a probabilistic broadcasting (CPB) system, the authors came up with an original method of disseminating data. As part of its clustering strategy, this method considers the directions in which cars are being driven. The built-in clustering structure adheres to a probabilistic forwarding approach concerning the distribution of data across cars.

**Ortiz et al., (2020) [20]** evaluate how well this technology functions in a city-wide mobility setting, with LoRa terminal devices installed in moving cars and a LoRa network serving as infrastructure. Moreover, the comparison of the simulated findings provided by NS-3 to those acquired through the communication connection between both the LoRa module within a car and a LoRa receiver. The packet delivery ratio (PDR), the time between packet receptions (PIR), and the received signal strength indicator (RSSI). Research in the field takes place at UFRJ, a Brazilian university located in Rio de Janeiro. The metrics analyzed in the simulated trials were found to agree with findings from the actual studies; however, the model is better by seeking a higher association with genuine experiments.

**Khattak et al., (2019) [21]** suggested that by improving network capabilities with LoRaWAN, not only the coverage increased but also lower the amount of power needed for IoT applications that use the network. Also,  the problems researchers run into when they try to use this integration, give them a way to learn more about the Veterinary and Comparative Orthopaedics and Traumatology (VCoT field). In the future, the expand on the current work to present a comprehensive framework that uses an architecture and design proof of concept to cover most aspects, such as the protocols and standards for facilities, communication systems, security, and privacy requirements, and various data protocols, as well as functional features, such as asset and resource management.

**Sherazi, et al., (2019) [22]** proposed a heterogeneous network architecture that takes advantage of the radio over fiber approach to establish context-aware network connectivity, incorporating multiple wireless interfaces installed on the on-board units (including wireless access in vehicular environments (WAVE), long-range wireless fidelity (WiFi), and fourth generation/long-term evolution (4G/LTE)). For VANETs to be scalable and adaptive for IoV providing a variety of emergency services, this heterogeneous network design is an effort to satisfy the needs of ubiquitous connection.

**Chiti et al., (2019) [23]** suggested a unique method for collecting information under time constraints in a typical network that is based on a token-passing system and is modified for wireless communications by establishing a virtual ring in which nodes are linked to both their predecessor and their successor. The suggested method, dubbed Tom Thumb, deals with the frequent topology shifts that are characteristic of VANETs. Tom Thumb is a decentralized protocol in which a token is sent from vehicle to vehicle and back to the starting point within a certain amount of time.

**Khattak et al., (2018) [24]** proposed an architectural framework for integrating VC with IoT to enable the delivery of new services and applications, such as IoT management through VC. The main interest of this is applications for smart cities that can be managed, controlled, and operated and vehicle networks. Insights into managing data in a resource-constrained, multi-paradigm setting are provided by this theoretical study. The difficulties that researchers have encountered when attempting to integrate such systems, such as those related to data collection, quality of data, security, privacy, scope, and so on. For the IoT-VC paradigm to become a reality, several obstacles must be overcome.

Table 1 summarised the reviewed literature from different authors' their techniques and outcomes were also described below:

Table 1: Comparison of the reviewed literature

|  |  |  |
| --- | --- | --- |
| **Authors** | **Techniques** | **Outcomes** |
| **Valente et al., (2023) [13]** | Federated learning | The Nano can fulfill numerous instances where services with softer standards might be deployed. |
| **Paredes et al., (2023) [14]** | FANET | Drone mobility shouldn't be compromised in the process of designing and selecting energy-gathering devices. |
| **Naeimipoor et al., (2022) [15]** | NCBR | Compared to the three clustering strategies, latency, packet delivery ratio, reliability, cost, and stability improved. |
| **Jeong et al., (2021) [16]** | DSRC | Situational, traffic signal-synchronized, emergency navigators, and elevated junction passing smart transportation applications and services. |
| **Soares et al., (2021) [17]** | Stochastic Petri net (SPN) model | RSU queues directly affect mean response time. |
| **Al-Khater et al., (2020) [18]** | Routing algorithms, Fuzzy logic, Machine learning, Data mining | Law enforcement organizations share internet criminal data for research while maintaining privacy. |
| **Fourati et al., (2020) [19]** | Clustering techniques | Compared to existing systems, higher content delivery ratio, low service latency and overhead, and more In Data. |
| **Ortiz et al., (2020) [20]** | LoRa terminal devices, Packet InterReception (PIR) | The simulated trials match the real experiments for all metrics. |
| **Khattak et al., (2019) [21]** | cloud computing, and the Internet of Things | LoRaWAN capacity boost improves coverage and energy efficiency. |
| **Sherazi, et al., (2019) [22]** | IoT, IoV | The suggested design provides the finest connection to meet customers' expectations often, servicing more clients. |
| **Chiti et al., (2019) [23]** | The token passing scheme, Tom Thumb (TT) | TT works well for smart city traffic monitoring and management. |
| **Khattak et al., (2018) [24]** | Vehicular clouds, IoT | The suggested architectural framework enables new and innovative IoT and VC applications. |

1. **Background study**

One of the most well-known and exciting developments in the field of intelligent transportation right now is the Vehicle Ad hoc Network (VANET). Despite this, VANET is subject to several vulnerabilities, one of which might lead to an incursion. In this research, an original approach to machine learning as a means of enhancing the performance of VANET is proposed. The suggested procedure is broken up into two stages. In Phase, I, Distributed Denial of Service (DDoS) assault is identified by using a cutting-edge machine learning strategy known as Support Vector Machine-Harris Hawks Optimization (SVM-HHO), which offers information on the automobile. Phase II lessens the damage caused by a DDoS assault and divides up available bandwidth using a tried-and-true method for managing resources that are based on an algorithm called the Hybrid Whale Dragonfly Optimization Algorithm (H-WDFOA). In conclusion, the suggested method was evaluated and contrasted with another conventional method. The solution that is being suggested at node 80 brings the drop value down to 0.15 while simultaneously bringing the delay time down to 15.64 seconds and the energy usage down to 2.0 mJ. These outcomes are evidence that the technique, which is presented, works well. Therefore, the suggested system is more effective than the ones that now exist [25].

1. **Problem formulation**

The wired connection protocols were built using standard approaches to operate the many interior components of the car using a single-designed system architecture. Because it uses wires, this strategy raises both the system and the maintenance costs of the car. Contemporary automotive networks make use of wireless protocols to transmit or receive data wirelessly inside or outside the vehicles to increase the cost efficiency of their operations. VANET is a relatively new and effective wireless technology that is being used in a variety of intelligent transportation networks. Although VANET is being created to allow efficient vehicle communication and the sharing of traffic information, VANET is also subject to a variety of security assaults, such as DOS attacks. It is extremely crucial to offer more secure and dependable communication between all the vehicles that are a part of the VANET system by detecting the assaults that are made on the system. In this research, a novel enhanced VANET paradigm is proposed for secure and reliable communication based on LoRa (Long Range) technology. Not only does this paradigm have improved throughput, latency rate, and bandwidth in comparison to other conventional methods, but it also helps mitigate the issues mentioned above.

1. **Research objectives**

* To develop a novel enhanced VANET paradigm for secure and reliable communication based on LoRa technology.
* To enhance the bandwidth of the communication system using an optimized path selection algorithm.
* To prove the robustness of the proposed model it is compared with another conventional method based on variables such as energy consumption, throughput, and many more.

1. **Research Methodology**

The concept of designed architecture is examined in the context of research methodology. The proposed model is operated on the traffic dataset. Then the seagull optimization is used to enhance the capacity of the nodes. An improved Deep Deterministic Policy Gradient (DDPG) algorithm is used to find the optimal path and finally, the efficiency of the model is evaluated.

1. **Technique used.**

Various techniques are used in the architectural design of the proposed model. these techniques are stated below:

* **Fuzzy Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS)**

In this research, TOPSIS is used to detect known attacks. It is now the method that is the most well-known for handling issues involving the use of many criteria in decision-making in this research TOPSIS is used for classifying DDoS attacks [26].

**The steps taken for fuzzy TOPSIS are as follows:**

**Step 1: Ratings should be given both to the conditions and the options.**

In the beginning, it proceeded on the assumption that the decision-making group consists of K members. The weight of the criteria is indicated by , and the fuzzy score of the selection maker on substitute concerning condition is defined as .

**Step 2: Evaluate the accumulated fuzzy ratings for the available options as well as the consolidated weights for each criterion.**

The weighted average fuzzy rating of the option concerning the criteria are calculated as follows: .

(1)

For each criterion , formulae are used to determine the aggregate fuzzy weight .

. (2)

**Step 3: Compute the results using the fuzzy decision matrix, which has been normalized.**

When calculating the normalized fuzzy decision matrix, is the formula to use,

Where,

and (3)

and (4)

**Step 4: Prepare the weighted normalized fuzzy decision matrix by performing the appropriate calculations.**

The fuzzy-weighted normalized decision matrix is where .

**Step 5: Calculate the Fuzzy Positive Ideal Solution (FPIS) and the Fuzzy Negative Ideal Solution (FNIS). Following are the calculations for FPIS and FNIS:**

where (5)

where (6)

**Step 6: Determine how far each alternative is from the FPIS and FNIS.**

The distance between each option and the FPIS and FNIS, respectively, should be specified as:

(7)

**Step 7: For each option, determine the similarity coefficient.**

The following formula is used to get the proximity coefficient for each option :

(8)

**Step 8: Rank all alternatives.**

The most advantageous option is one with the greatest proximity coefficient [26].

* **Seagull optimization**

The maximum capacity of the nodes in the communication has been achieved via the use of the seagull optimization method. The Seagull optimization mimics the behaviour of seagulls, which are used for hunting and migrating. To avoid running across one other, they travel in separate groups that all begin in distinct places. The seagulls rearrange themselves according to who has the greatest chance of surviving [27]. Figure 4 shows the hunting procedure of a seagull by performing the migration and attacking method.

Diagram

Description automatically generated

Figure 4: Seagull technique [27]

* **Deep Deterministic Policy Gradient (DDPG) Algorithm**

A DDPG technique for route selection and optimization is implemented in the proposed methodology. Deterministic policy gradient and deep-Q networks come together to form the DDPG method. The DDPG method is employed in the recurrent learning process, which does not need a model. Where route selection is continuous rather than discrete, like in a VANET system, this capability is useful [28]. Figure 5 shows the block architecture of the DDPG algorithm.

Actor

Value Function

Policy

State

Action

Environment

Reward

TD error

Critic

Figure 5: DDPG method [29]

1. **Proposed algorithm.**

**Start**

1. Read traffic dataset as input variable → T, DDPG→ Deep Deterministic Policy Gradient

2. Perform Data pre-processing on → T

3. Split →T as → A, B \\ A→ Train set..., B→ Test set

4. Train → TOPSIS on → T (A) then,

5.Test → TOPSIS on → T (B)

6. If DDoS is detected

End the process.

7. Else,

Initialize the no. of nodes based on → QoS,

End for

8. Apply Seagull optimization to → enhance node capacity

9. Evaluate node fitness based on → QoS

10. Select the shortest route using → DDPG

11. Apply optical routing bursting and → packet transferring

12. Evaluate model performance based on→ Metrics (Throughput, Latency rate, End to End delay)

**End**

1. **Proposed methodology.**

The flowchart of the proposed architecture is discussed in the context of the proposed methodology with the help of block representation as shown in figure 6. further the architecture is discussed in detail for better understanding.

Traffic dataset

Initialize the number nodes with QoS parameters.

TOPSIS based training and testing.

Data preprocessing

QoS based fitness evaluation.

DDoS detection

Route selection using DDPG algorithm.

Seagull optimization for enhancing node capacity.

Evaluation metrics

Applying optical routing bursting

Packet transferring

Figure 6: Illustration of the proposed model

**Following are the steps that describe the proposed model:**

**Step 1: data collection and pre-processing**

At the beginning of the process, the traffic dataset is considered which is easily available on the website of Kaggle. Because the network data from VANET is so large, after the dataset has been gathered, it is forwarded for pre-processing. As a result, data pre-processing can identify and remove redundant and duplicate data in network traffic.

**Step 2: TOPSIS model training and testing**

After the data collection and data pre-processing in this step the training and testing of the proposed model are performed using the TOPSIS model. For train and testing, the dataset is divided into two sets 70 percent is used for training and 30 percent is used for testing. After the training, the model testing is performed in which DDoS is detected.

**Step 3: Initialization based on QoS.**

In step 3, after the detection of DDoS, the number of nodes is initialized based on QoS parameters to allocate the shortest path for channel communication.

**Step 4: Seagull optimization**

After the initialization of nodes based on QoS in this step to enhance the capacity of the nodes, the seagull optimization is performed.

**Step 5: QoS-based fitness evaluation.**

In step 5, after enhancing the capacity of the nodes using seagull optimization the fitness of the nodes is evaluated based on QoS parameters.

**Step 6: Route selection**

After evaluating the fitness values base on QoS in this step the route selection is performed. For efficient data routing the route selection is performed using the DDPG algorithm.

**Step 7: Applying optical routing bursting and packet transferring.**

In step 7, after selecting the optimized path for data routing the optical routing busting is applied, and then the data transferring between the nodes is performed. And finally, the efficiency of the model is evaluated based on Evaluation metrics such as power consumption, throughput, and many more.

1. **Results and discussion**

In this section results are discussed in detail that are obtained after the implementation of the proposed architecture. Initially, an improved fuzzy approach known as TOPSIS was used to detect the DDoS assault by utilising data on the vehicles involved. Table 3 demonstrates that the suggested TOPSIS strategy based on modified fuzzy system performs better than state-of-the-art methods. Then in second stage, the proposed model is compared with other conventional method to investigate the superiority of the proposed model.

* **Dataset**

In this section, the dataset that is used in the research methodology is generated from primary sources and simulated from Network Simulator (NS2) software. It is split into the percentage of 30 and 70. First 70% data is used to train the proposed model then the 30% data is used to test the model. Table 2 shows the system configuration and the tool used for simulation.

Table 2 Configuration of simulation

|  |  |
| --- | --- |
| **System** | **Configuration** |
| Tool | NS2, MATLAB |
| Computer | Windows10 pro |
| Processor | Intel core i5 2.70GHz |
| RAM | 8+8 GB |
| Type | X64 based processor |

1. **Performance metrics**

* **Throughput**

The throughput parameter characterises the ratio between the total number of packets produced by the transmitting node in each time interval and the total amount of data established by the recipient node in packets. Visualized as:

(1)

Where, RP received packet, TP is the transmission period.

* **Packet delivery ratio (PDR)**

This is a technique for doing speedy analysis of data packets moving through and leaving a network. It is computed by dividing the total number of packets sent by the source by the total number of packets collected by the vehicle. To determine the PDR, we use the following formula:

(2)

Where, GP is the generated packets.

1. **Performance evaluation**

In this section, the effectiveness of the strategies that have been offered in terms of criteria like power consumption, data transfer rate (bits per second), network longevity, and PDR is discussed. Table 3 shows the obtained values of various efficiency evaluating parameters to show the performance of the proposed architecture. In the first stage, an improved fuzzy approach known as TOPSIS was used to detect the DDoS assault by utilising data on the vehicles involved. To evaluate the model's potential to detect DDoS assaults and properly allot bandwidth in VANET scenarios, performance metrics were largely employed.

Table 3 Proposed method’s performance at different no. of nodes.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Node** | **Energy consumption** | **Throughput** | **Network lifetime** | **PDR** |
| 20 | 0.08 | 1350 | 140 | 25 |
| 40 | 0.19 | 2000 | 660 | 39 |
| 60 | 0.24 | 1770 | 440 | 50 |
| 80 | 0.36 | 1390 | 200 | 65 |
| 100 | 0.49 | 1230 | 90 | 73 |

* **Energy consumption**

Figure 7 illustrates the total amount of energy that would be consumed by the suggested method. The rate of energy consumption of each node is stated below based on the information in table 3, which can be found here. At node 20, 40, 60, and 80, as well as at node 100, the respective energy consumption is habited to be 0.08, 0.19, 0.24, 0.36, and 0.49. The increased number of nodes is followed by an increase in the amount of energy that is used.

Chart

Description automatically generated

Figure 7 Consumption of energy

Figure 8 depicts the recommended method's energy consumption ratio depending on data rates. The energy consumption of the proposed approach is evaluated at different data packet rate such as 4, 6, 8, 10, 12, and 14 and the results shows that if data packet rate is high then it indicates an energetic peak; otherwise, lesser data rates result from the same amount of energy.

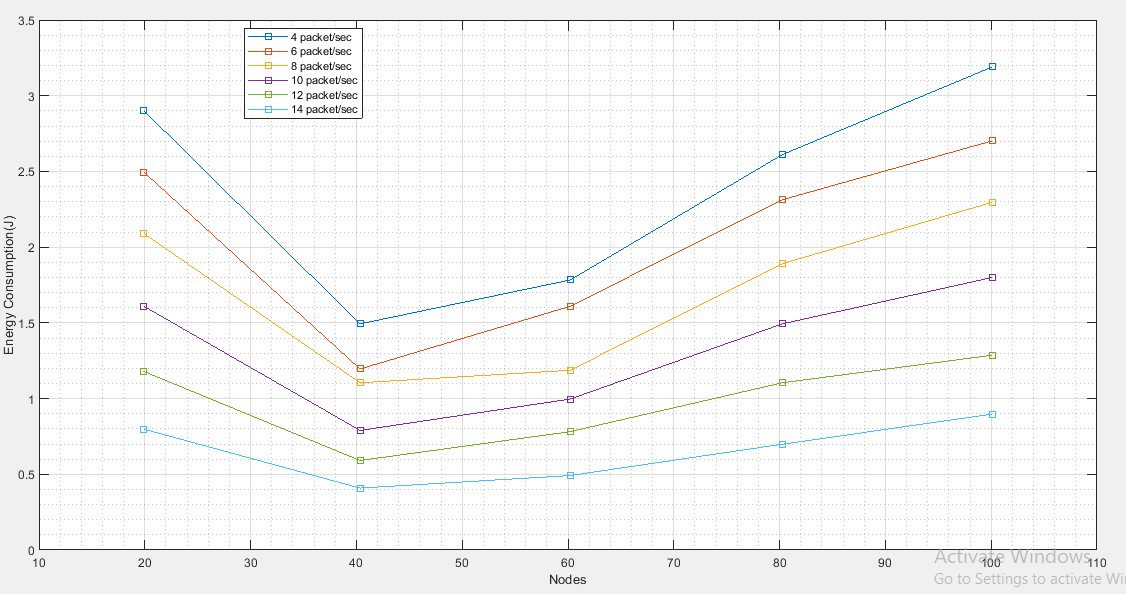


Figure 8 consumption of energy at different data packets

* **Network lifetime**

Figure 9 shows the overall network lifetime of the proposed architecture at different no. of nodes in a graphical manner. Table 3 shows that the network lifetime of proposed model at 20, 40, 60, 80, 100 nodes is 140, 660, 440, 200, 90 respectively. The rise in the number of nodes was matched by a corresponding rise in the network's lifetime.

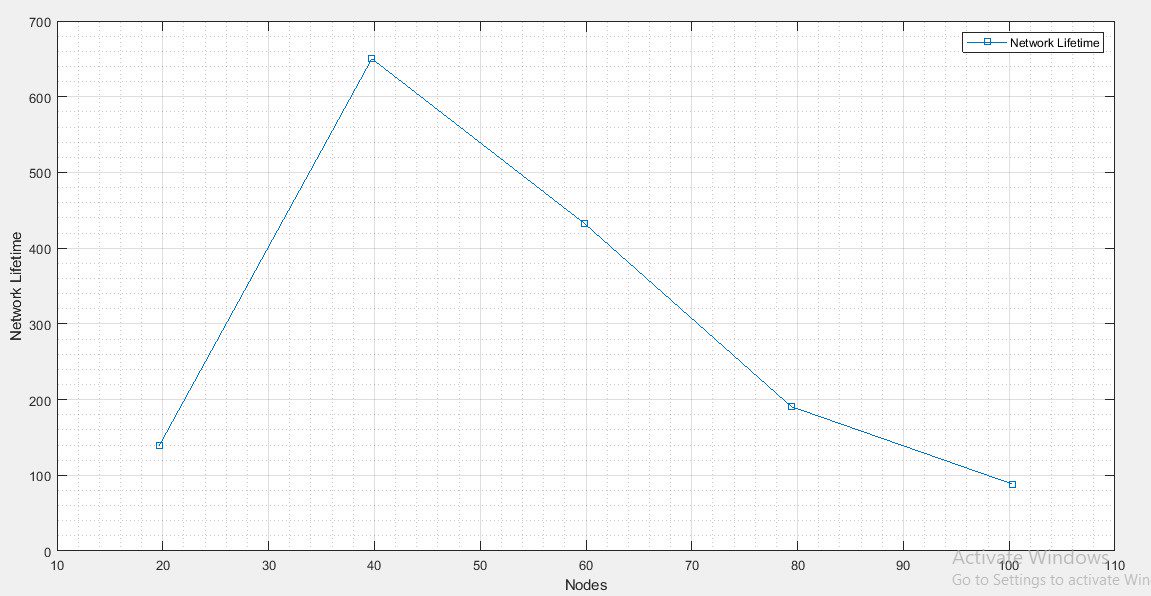


Figure 9 Network lifetime

Figure 10 shows the network lifetime at different data packets rate. The network lifetime of the proposed approach is evaluated at different data packet rate such as 4, 6, 8, 10, 12, and 14 and the results shows that at low data packet rate the network lifetime appears high and vice versa.

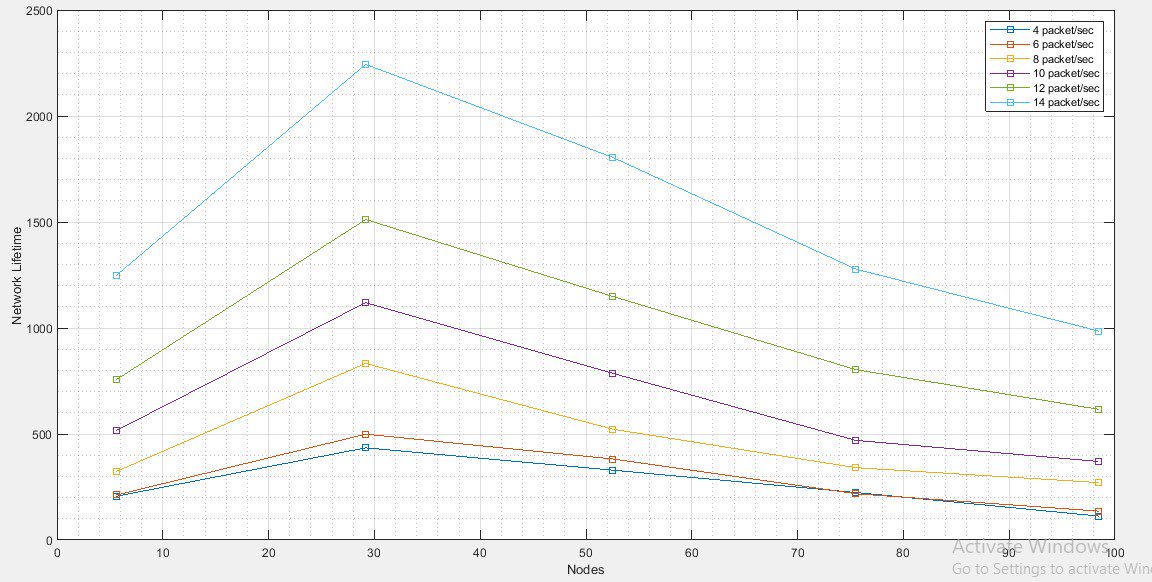


Figure 10 Network lifetime at different data packet transferring.

* **Throughput**

Figure 11 shows the overall throughput of the proposed architecture at different no. of nodes in a graphical manner. Table 3 shows that the throughput of proposed model at 20, 40, 60, 80, 100 nodes is 1350, 2000, 1770, 1390, 1230 respectively.

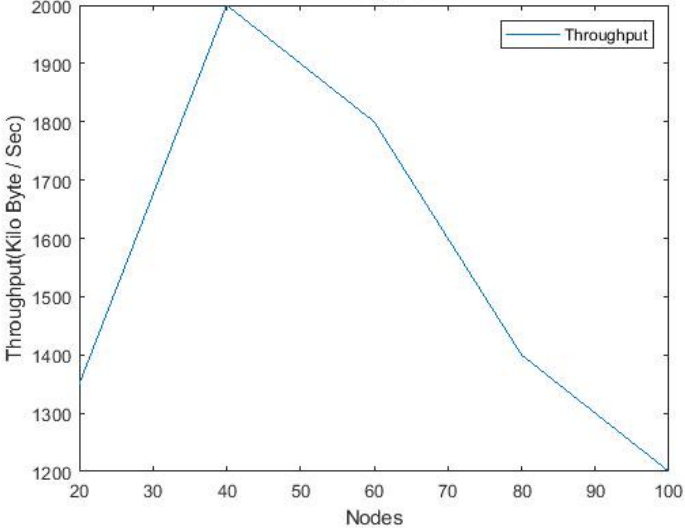


Figure 11 Throughput

Figure 10 shows the network lifetime at different data packets rate. The network lifetime of the proposed approach is evaluated at different data packet rate such as 4, 6, 8, 10, 12, and 14 and the results shows that when the data packet rates were low, the throughput ratio would likewise drop.

Chart, line chart

Description automatically generated

Figure 12 Throughput at different data packet transferring.

* **Packet delivery ratio**

To maximise the efficiency of both arriving and departing network traffic, the PDR was analysed and assessed. Under the context of VANET, the PDR is indicative of the system's overall higher presentation. Figure 13 shows the PDR of the proposed architecture at different no. of nodes in a graphical manner. Table 3 shows that the throughput of proposed model at 20, 40, 60, 80, 100 nodes is 25, 39, 50, 65, and 73 respectively.

Chart, line chart

Description automatically generated

Figure 13 PDR

* **Comparative analysis based on no. of node.**

In the second stage, the proposed model is compared with other existing technique based on various parameters to evaluate the superiority of the proposed model. The primary objective of these performance measurements was to conduct an analysis of the recommended model's ability to make mobility predictions within VANET. Figure 14 shows the performance of proposed model and existing model on various performance measuring parameters with respect to different number of nodes. The obtained results demonstrated that the value of delay, energy consumption, drop, throughput, and fairness index at node 20 is 0.245, 6, 0.5854, 42,889, and 60 respectively, at node 40 is 10.8954, 2, 0.1458, 30,787 and 11 respectively, at node 60 is 13.8547, 1.874, 0.1214, 34,465 and 13 respectively, at node 80 is 13.9987, 1, 0.1356, 42,548 and 12 respectively. The obtained results shows that the proposed model performed better than other conventional method.

|  |  |
| --- | --- |
|  |  |
| (a) Delay | (b) Energy consumption |
|  |  |
| (c) Drop | (d) Throughput |
|  | |
| (e) Fairness index | |
| Figure 14 Comparison based on no. of nodes. | |

* **Comparative analysis based on varying speed parameters.**

In this analysis the proposed model is compared with other conventional method in terms of varying speed parameters with performance measuring parameters such as delay, energy consumption, drop and throughput. Figure 14 shows the performance of proposed model and existing model in graphical manner on various performance measuring parameters with respect to varying speed parameters such as 20, 40, 60 and 80. The obtained results demonstrated that the value of delay, energy consumption, drop, throughput, and fairness index at speed 20 is 80.2465, 1280, 11.4578, 220, and 2.7458 respectively, at speed 40 is 305.154, 590, 6.8514, 30, and 1.9547 respectively at speed 60 is 832.258, 800, 8.1578, 20, and 0.957 respectively, at speed 80 is 1184.2545, 1160, 10.4587, 14, and 0.978 respectively. The obtained results shows that the proposed model performed better than other conventional method.

|  |  |
| --- | --- |
|  |  |
| (a) Delay | (b) Energy consumption |
|  |  |
| (c) Drop | (d) Throughput |
|  | |
| (d) fairness index | |
| Figure 15 Comparison based on varying parameters. | |

1. **Conclusion and future scope**

Vehicle communication and traffic information are being improved by VANET. VANET security concerns include DoS attacks. Identifying system assaults is crucial to improving VANET vehicle communication security. In this research, a novel enhanced VANET paradigm is proposed for secure and reliable communication based on LoRa technology. An updated fuzzy approach called TOPSIS was used to detect the DoS assault in this study. After that, seagull optimization boosts node capacity. Finding the best path requires an enhanced DDPG method. finally, the model is compared against other approaches to assess its efficacy. The obtained results show that at node 60, the value of delay, energy consumption, and drop, is 13.8547, 1.874, and 0.1214 respectively which is better than any other existing techniques. In future work, the study will analyse how driver behaviour and road conditions affect VANET performance and simulate proposed model for real-world situations to overcome network real-time limits.

**References**

Al-Khater, Wadha Abdullah, Somaya Al-Maadeed, Abdulghani Ali Ahmed, Ali Safaa Sadiq, and Muhammad Khurram Khan. "Comprehensive review of cybercrime detection techniques." IEEE Access 8 (2020): 137293-137311.

Poongodi, M., Mounir Hamdi, Ashutosh Sharma, Maode Ma, and Pradeep Kumar Singh. "DDoS detection mechanism using trust-based evaluation system in VANET." IEEE Access 7 (2019): 183532-183544.

ur Rehman, Sabih, M. Arif Khan, Tanveer A. Zia, and Lihong Zheng. "Vehicular ad-hoc networks (VANETs)-an overview and challenges." Journal of Wireless Networking and Communications 3, no. 3 (2013): 29-38.

Al-Khater, Wadha Abdullah, Somaya Al-Maadeed, Abdulghani Ali Ahmed, Ali Safaa Sadiq, and Muhammad Khurram Khan. "Comprehensive review of cybercrime detection techniques." IEEE Access 8 (2020): 137293-137311.

Saggi, M. K., and R. K. Sandhu. "A survey of vehicular ad hoc network on attacks and security threats in vanets." In International Conference on Research and Innovations in Engineering and Technology (ICRIET 2014), pp. 19-20. 2014.

Hussain, Rasheed, Zeinab Rezaeifar, and Heekuck Oh. "A paradigm shift from vehicular ad hoc networks to VANET-based clouds." Wireless Personal Communications 83 (2015): 1131-1158.

Amjid, Ayesha, Abid Khan, and Munam Ali Shah. "VANET-based volunteer computing (VBVC): A computational paradigm for future autonomous vehicles." IEEE Access 8 (2020): 71763-71774.

Al-Sultan, Saif, Moath M. Al-Doori, Ali H. Al-Bayatti, and Hussien Zedan. "A comprehensive survey on vehicular ad hoc network." Journal of network and computer applications 37 (2014): 380-392.

Reis, Andre B., Susana Sargento, Filipe Neves, and Ozan K. Tonguz. "Deploying roadside units in sparse vehicular networks: What really works and what does not." IEEE transactions on vehicular technology 63, no. 6 (2013): 2794-2806.

Eckhoff, David, Falko Dressler, and Christoph Sommer. "SmartRevoc: An efficient and privacy preserving revocation system using parked vehicles." In 38th Annual IEEE Conference on Local Computer Networks, pp. 827-834. IEEE, 2013.

Ayoub Kamal, Muhammad, Muhammad Mansoor Alam, Aznida Abu Bakar Sajak, and Mazliham Mohd Su’ud. "Requirements, Deployments, and Challenges of LoRa Technology: A Survey." Computational Intelligence and Neuroscience 2023 (2023).

Gallego-Madrid, Jorge, Alejandro Molina-Zarca, Ramon Sanchez-Iborra, Jorge Bernal-Bernabe, José Santa, Pedro Miguel Ruiz, and Antonio F. Skarmeta-Gómez. "Enhancing extensive and remote lora deployments through mec-powered drone gateways." Sensors 20, no. 15 (2020): 4109.

Valente, Renato, Carlos Senna, Pedro Rito, and Susana Sargento. "Embedded Federated Learning for VANET Environments." Applied Sciences 13, no. 4 (2023): 2329.

Paredes, William David, Hemani Kaushal, Iman Vakilinia, and Zornitza Prodanoff. "LoRa Technology in Flying Ad Hoc Networks: A Survey of Challenges and Open Issues." Sensors 23, no. 5 (2023): 2403.

Naeimipoor, Farzaneh. "An emergency vehicle prioritization protocol for VANET based on QoS." PhD diss., Université d'Ottawa/University of Ottawa, 2022.

Jeong, Hwanseok Harrison, Yiwen Chris Shen, Jaehoon Paul Jeong, and Tae Tom Oh. "A comprehensive survey on vehicular networking for safe and efficient driving in smart transportation: A focus on systems, protocols, and applications." Vehicular Communications 31 (2021): 100349.

Soares, André, and Francisco Airton Silva. "Performance evaluation of smart cooperative traffic lights in VANETs Laécio Rodrigues, Firmino Neto, Glauber Gonçalves."

Al-Khater, Wadha Abdullah, Somaya Al-Maadeed, Abdulghani Ali Ahmed, Ali Safaa Sadiq, and Muhammad Khurram Khan. "Comprehensive review of cybercrime detection techniques." IEEE Access 8 (2020): 137293-137311.

Fourati, Lamia Chaari, Mohamed Ali Ben Rejeb, and Samiha Ayed. "New ICN based Clustering Mechanism for Vehicular Networks." In 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA), pp. 1-4. IEEE, 2020.

Ortiz, Fernando M., Thales T. de Almeida, Ana E. Ferreira, and Luis Henrique MK Costa. "Experimental vs. simulation analysis of LoRa for vehicular communications." Computer Communications 160 (2020): 299-310.

Khattak, Hasan Ali, Haleem Farman, Bilal Jan, and Ikram Ud Din. "Toward integrating vehicular clouds with IoT for smart city services." IEEE Network 33, no. 2 (2019): 65-71.

Sherazi, Hafiz Husnain Raza, Zuhaib Ashfaq Khan, Razi Iqbal, Shahzad Rizwan, Muhammad Ali Imran, and Khalid Awan. "A heterogeneous IoV architecture for data forwarding in vehicle to infrastructure communication." Mobile Information Systems 2019 (2019).

Chiti, Francesco, Romano Fantacci, Francesca Nizzi, Laura Pierucci, and Carlos Borrego. "A distributed token passing protocol for time constrained data gathering in VANETs." Electronics 8, no. 8 (2019): 823.

Khattak, Hasan Ali, Rasheed Hussain, and Zoobia Ameer. "Internet of vehicles: Integrated services over vehicular ad hoc networks." In Smart Societies, Infrastructure, Technologies and Applications: First International Conference, SCITA 2017, Jeddah, Saudi Arabia, November 27–29, 2017, Proceedings 1, pp. 61-73. Springer International Publishing, 2018.

Marwah, Gagan Preet Kour, Anuj Jain, Praveen Kumar Malik, Manwinder Singh, Sudeep Tanwar, Calin Ovidiu Safirescu, Traian Candin Mihaltan, Ravi Sharma, and Ahmed Alkhayyat. "An Improved Machine Learning Model with Hybrid Technique in VANET for Robust Communication." Mathematics 10, no. 21 (2022): 4030.

Nădăban, Sorin, Simona Dzitac, and Ioan Dzitac. "Fuzzy TOPSIS: a general view." Procedia computer science 91 (2016): 823-831.

Lei, Gang, Heqing Song, and Dragan Rodriguez. "Power generation cost minimization of the grid-connected hybrid renewable energy system through optimal sizing using the modified seagull optimization technique." Energy Reports 6 (2020): 3365-3376.

Nahar, Ankur, and Debasis Das. "SeScR: SDN-enabled spectral clustering-based optimized routing using deep learning in VANET environment." In 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA), pp. 1-9. IEEE, 2020.

Fan, Luqin, Jing Zhang, Yu He, Ying Liu, Tao Hu, and Heng Zhang. "Optimal scheduling of microgrid based on deep deterministic policy gradient and transfer learning." Energies 14, no. 3 (2021): 584.