Iranian Journal of Fuzzy Systems

Volume 21, Number 6, (2024), pp. 15-31

Original paper

University of Sistan and Baluchestan

A fuzzy based efficient and blockchain oriented secured routing in vehicular Ad-Hoc networks

N. G. Praveena[1], K. Selvaraj[2], T. Kalaiselvi[3], Srigitha S. Nath[4] and D. Prabakaran[5]

[1] *Department of Electronics and Communication Engineering, R.M.K. College of Engineering and Technology, Chennai, India*
[2] *Department of Information Technology, PSNA College of Engineering and Technology, Dindigul, India*
[3] *Department of Artificial Intelligence and Data Science,Easwari Engineering College, Chennai, India*
[4] *Department of Electronics and Communication Engineering, Saveetha Engineering College, Chennai, India*
[5] *Department of Electronics and Communication Engineering, IFET College of Engineering, Villupuram, India*

drpraveenang@gmail.com, selme04@gmail.com, kalaiselvi.t@eec.srmrmp.edu.in
srigithapramodh@gmail.com, dprabakaranmtech@gmail.com

Abstract

Vehicular ad-hoc networks (VANET) represent an improved iteration of Wireless Sensor Networks (WSN) with mobile sensory nodes situated within vehicles. The Vehicular Adhoc Networks hold a crucial position within smart city applications as inter-vehicle communication is deemed indispensable for maintaining the technological efficiency of the city. Despite the benefits provided by VANET, it encounters numerous challenges and drawbacks within the context of smart city applications. One such challenge pertains to the security and privacy principles of VANET. Privacy and security emerge as principal concerns associated with VANET, prompting multiple researchers to propose security solutions over the past decade. The present research endeavor focuses on elevating the quality of service (QoS) by offering an enhanced level of security for data communication. This security enhancement is achieved through the use of blockchain technology and the integration of Elliptical Curve Cryptography with secure hash functions to safeguard data communication from node to Mobile Control Unit (MCU). Furthermore, the proposed research work presents an efficient routing mechanism for data between mobile nodes and the Control Unit by employing neuro fuzzy logic to identify the optimal path from the source node to the Mobile Control Unit (MCU). The proposed work is compared with existing cryptographic methodologies as well as state-of-the-art routing path optimization algorithms, namely Particle Swarm Optimization (PSO), Genetic Algorithm (GA), Memetic Algorithm (MA), and Honey Bee Optimization (HBO), in order to establish its superiority in terms of computational time, throughput, packet delivery ratio, and accuracy.

Keywords: Vehicular Adhoc networks, wireless sensor networks, elliptical curve cryptography, particle swarm optimization (PSO), genetic algorithm (GA), memetic algorithm (MA), honey bee optimization (HBO) algorithm.

1 Introduction

The emergence of the Internet of Things (IoT) and the anticipation of implementing advanced technologies in day to day life, paves path to the introduction of smart devices or smart systems for various applications. Smart city is one such notable application, employs the information and communication technologies to enhance the functional efficiency, quality of the governance and user satisfaction. The predominant objective of the smart city is to enhance the quality of the service rendered to the users through the services like social economic quality, sustainability, better level of inter-connectivity, sustainability, waste management, traffic management and pollution control etc. One of the major evolutions in the smart city is the traffic management system, as it remains to be the major challenge in most cities during the peak transition period. As a significant unit of the smart city, an Intelligent Transportation System

Corresponding Author: N. G. Praveena
Received: February 2024; Revised: November 2024; Accepted: December 2024.
https://doi.org/10.22111/ijfs.2024.48069.8461

(ITS) [24] is considered as the key technology for enhancing the user satisfaction, mitigating the road traffic congestion, road safety and for providing significant level of efficiency in terms of transportation sector. The use of ITS broadens beyond information, control, and monitoring of road congestion to including safe driving and effective exploitation of the infrastructure supporting transport systems. In addition to improving traffic supervision and organization, improving the driving expertise, and providing soothe to drivers and passengers. VANET [2] is a vital technology and a subclass of mobile Ad-hoc networks, can offer other priceless services in smart cities that require network connectivity. As shown in Figure 1, a VANET typically consists of vehicles, Road Side Units (RSUs), Monitoring and Control Units (MCUs).

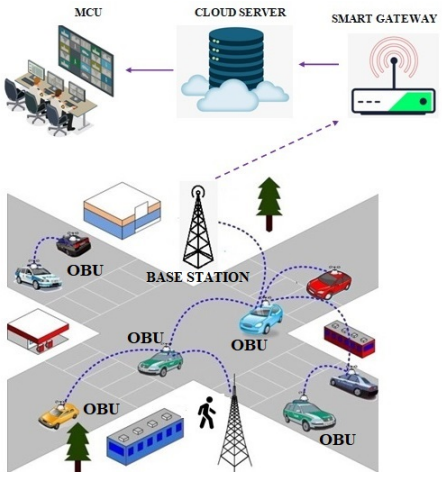


Figure 1: Proposed VANET architecture for secure and QoS enhanced communication.

Each vehicle has an On-Board Unit (OBU) built into it, enabling communication with MCU. The RSUs installed on the sides of roads are wireless network devices that can provide vehicles with traffic-oriented services such as wireless connectivity, data communication between the vehicles and MCU through the smart gateway and cloud server. Apart from the aforementioned parties involved in the active functioning of the VANET, a trusted Third Party Authenticator (TPA) [19] is involved in generating and sharing the key among the vehicular users. The MCU is a control unit that accumulates traffic data from RSUs, evaluates it, and utilizes the findings to recommend diversified actions and solicit feedback. VANET [10] uses Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. A Dedicated Short-Range Communication (DSRC) protocol is employed by vehicles or OBUs [15] to communicate with one another and communicate the data based on vehicle traffic among the nearer RSUs. Even when vehicles are moving at a high rate of drift, the DSRC facilitates data communication covering a small distance. The OBU is anticipated to transmit traffic-related data to nearby OBU or RSU [7] in a time space of not less than 100 ms. As per the design of DSRC protocol, which implement the IEEE 802.11p principles [13] for Wireless Access in Vehicular Environments (WAVE), communicates the road traffic related information from the OBU to the MCU through the smart gateway. Vehicles can use this information to make proactive decisions that will help them avoid accidents, traffic jams, and disasters. In order to offer the required supervision and control actions, the RSUs send traffic based data to the Traffic Management Control (TMC) or Trusting Authority (TA) such as a crash warning and an emergency traffic light control. The homogenous type of message is produced by all OBU (vehicles) when the population of the OBU is taken into account, and it is sent to the MCU via smart gateways and the cloud server. The communication from the vehicle to vehicle or from vehicle to the Main Control Unit [12] is performed on the Wireless Sensor Networks background with dynamic nodes, capable for moving from one place to another. The major challenges experienced in this proposed work are as follows.

i. No constant routing algorithm shall be implemented due to the dynamic nature of the sensor nodes (OBU).

ii. The data transmitted between the OBU to OBU and OBU to MCU is insecure, as the data communication is performed in the open network.

Despite of solutions offered by various researchers, the aforementioned challenges prolonged to exist proving the open channel is vulnerable to the attackers. This threat arises due to the openness of the channel in the VANET environment, which motivates the hackers to acquire the message, involving in active and passive attacks of observing the data pattern and mostly resulting in modification or deletion of the transmitted message from one OBU to another

OBU or to MCU. To prove the significance of this concern and to highlight the serious effects of this attack, consider that the vehicle identity is disclosed over insecure channel and the message are transmitted in the form of plain text to other OBU or MCU, the hacker tends to acquire the plain text illegally and shall gain knowledge on the travel pattern of an individual by tracking their vehicle. This may also leads to illegal activities like kidnapping, assassination of celebrities and high profile personalities. To overcome these concerns, it is necessary to communicate among the OBU/MCU in an encrypted format [31]. The encryption and decryption process shall not be directly implemented in the VANET environment [30], as the infrastructure is not suitable to handle.

This research manuscript is organized with a detailed analysis on recent related works in Section 2 to identify the setbacks by which the objectives of the proposed work have been framed. The proposed work is illustrated in Section 3 followed by a detailed performance and security analysis in the Section 4. The research manuscript is concluded highlighting the merits and introducing the future scopes of research in Section 5.

1.1 Contributions of the proposed work

The evolution of smart cities anticipates smart systems to be incorporated for a better management of traffic and to monitor the activities of all vehicles inside the city. In this regard, this proposed work on successful implementation will offer the following contributions to the society.

i. Offers Secure and efficient transit of vehicles in and out of the smart city. The information related to the vehicles were maintained safer and all the vehicles need to be authenticated before entering into the city. This process enhances the security of the city and prohibits vehicles with fake identity from entering into the city and involving in anti-social activities.

ii. The proposed work offers a better communication path using the fuzzy logic, by considering the present traffic related information.

2 Literature review

VANET is an emerging technology with abundant challenges and opportunities for technological development thus attracts various researchers to involve in identifying solutions for the aforementioned challenges. Varieties of solutions have been proposed by various researchers and some of the notable research results were listed here which acts as the motivational factor for this research.

K. Kandali and et al. (2021) introduced a novel clustering based routing protocol integrated with the K-Means clustering process [14] to provide an efficient data transmission between two vehicles in the VANET. The K-Means clustering algorithm performs the cluster of dynamic sensor nodes and assisted in efficient routing process. The introduced method offered a better level of throughput in performing data communication, despite lags in the security aspect of the data. Z.Hassan and et al. (2020) proposed a scheme [9] to detect the black hole detection in the VANET. The author employed four vital parameters including the hop count, sequence number, packet delivery ratio, and propagation delay to design the proposed model. The analysis of the proposed model exhibits better level of security, on the other hand experienced a major packet loss during the data transmission.

J. Shen and et al. (2017) had proposed a novel routing protocol with trustworthy feature named Trustworthiness Evaluation based Routing Protocol (TERP) [22] in the VANET application. This protocol was introduced to enhance the security of the data transmitted in the VANET application. The proposed work enhanced the security level along with the packet delivery ratio by mitigating the overhead of the communication process. G. D. Singh and et al. (2022) had implemented an hybrid Genetic algorithm and Firefly algorithm to generate an Hybrid Genetic Firefly algorithm (HGFA) [23] to perform a faster data communication in the VANET environment. The performance analysis yield a data delivery ratio of 77% when compared with the existing optimization algorithms.

Y. Wang and et al. (2021) has introduced an All Round and High Privacy Preserving Location based Routing (ARPLR) algorithm [27] to perform a location based energy efficient and secured routing in the VANET application. The system introduces an elevated level of security in the data communication by performing encryption and decryption process during the data transmission process. In addition, the system offered a better level of packet delivery ratio and exhibited an elevation of 30% when compared to the existing VANET algorithms. A.M.R.Tolba (2018) had proposed a Trust Oriented Distributed Authentication (TDA) system [25], depends on the global trust server to provide an enhanced level of security to the VANET communication. In addition to the security, the proposed system intends to provide a better level of routing efficiency in data communication process. The proposed TDA results in enhanced level of security by enhancing the recognition rate of the data broadcasting.

M. S. Haghighi and et al. (2019) had proposed a novel onion based routing protocol [21] with an objective to perform an efficient and secured routing of data from the OBU to the base station. The proposed protocol offered a better level of anonymity in source, destination and in routing processes. The performance evaluation of the proposed protocol offered a better level of security with the median packet delivery ratio despite of increased retransmission of data. P. Upadhyay and et al. (2022) had introduced an enhanced hybrid Glow warm optimization algorithm [26] for the traffic awareness in the VANET environment. This proposed work was implemented to enhance the level of the data security and to perform an energy efficient routing in the mobility environment. The performance analysis offered a better level of security, despite due to the increase in volume of data, experienced a mitigated efficiency in routing process.

C. Chen and et al. (2019) had proposed a Road Weight Evaluation (RWE) algorithm [3] to overcome the delay concern experienced during the data communication in the VANET environment. The proposed RWE algorithm aims in determining the optimal routing path to reach the Grid Zones (GZ) through which the data is communicated to mitigate the transmission delay and to enhance the packet delivery ratio. M. H. Eiza and et al. (2015) had introduced a secure QoS routing algorithm in the VANET environment with an objective to reduce the propagation delay and to enhance the Quality of Service. To achieve this objective, the author employed the Ant Colony Optimization (ACO) [8] algorithm to detect the suitable path from the vehicle to the base station. The simulation analysis of the proposed work proved with a mitigated propagation and end to end delay along with enhanced packet delivery ratio.

2.1 Limitations of the existing methodologies

Based on the study performed, and from the various sources, the following challenges were observed to be existing in the present VANET technology.

i. Existing algorithms provide either security of an increased QoS in the VANET environment, thus concentrates on any one of the parameter.

ii. The security algorithms enhanced the load of the data transmission, which is directly influencing the delay in the data communication process.

iii. The routing algorithm employed in the mobility environment is identified to be inefficient in terms of delay, throughput and packet delivery ratio. This necessitates the identification of a suitable routing algorithm.

2.2 Objectives of the proposed work

With knowledge on the aforementioned limitations of the existing VANET methodologies, the following objectives have been framed so that the proposed work is aimed to achieve the intended beneficiaries.

i. To implement a fuzzy based routing algorithm in the mobility environment to offer a better level of throughput, packet delivery ratio, mitigated overhead and end to end delay.

ii. To implement the blockchain technology, so that to enhance the level of security in maintaining the data related to the incoming vehicles.

3 Proposed methodology

3.1 Preliminaries

The fuzzy neural system [18] employed in the proposed work is the integrated version of the fuzzy logic and neural networks, in which the fuzzy logic is controlled by various weights in the hidden layers. The input, output and the hidden layers are considered as the neurons whereas the fuzzy rules are applied to the hidden layers to determine the solution for the incoming objective function. The first layer is the input layer followed by the fuzzification process in the layer 2. The layer 3 is fed with the fuzzy rules to perform the defuzzification process in the layer 4. The final decision output is achieved in the layer 5 as depicted in Figure 2. Assume an ECC for secure key generation using the mathematical relation represented in following equation.

$$y^2 = x^3 + px + q.$$

The points on the elliptic curve Ec with a cyclic group G in the order ‘a’ and generator ‘g’.The‘x’ and ‘y’ are the coordinates of the elliptical curve while ‘p’ and ‘q’ are the cyclic groups.

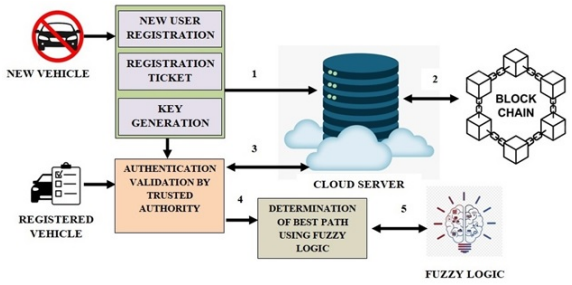


Figure 2: Schematic representation of proposed work.

i. Assumption: Consider two points $P1, P2 \epsilon G$, where $P2 = rP1$ and $r = ZG$ and is computationally feasible to determine the r using the point 'G' in the elliptic curve. The terms P1, P2 are the points in the elliptical curves, of the cyclic group 'G' and Z is the random value chosen to determine the radius of the curve.

ii. The Elliptical Curve Cryptography (ECC) is the public key cryptography, assists in performing the secure key communication process. In the proposed work, the secure key generated by the incoming vehicle is communicated with the authenticated server for validation purpose.

3.2 Proposed model

The proposed model is capable of performing communication between V2V which were equipped with the GPS module for the purpose of identifying the location and time information of vehicle. The clock frequency of the GPS module placed in all vehicles are considered to be synchronized and as described in the previous section, the OBU and MCU were implicit to be completely reliable units with sufficient resources. The trust of the OBU and the MCU is verified by the Trusting Authority (TA), and the disputes risen is cleared using the Dispute Resolving Agent (DRA).The MCU is known for its trustworthy while the OBU has to undergo the trust validation process with the TA. The proposed work incorporates the blockchain to hold the chain of data related to the vehicle and is composed of phases, namely the initialization phase, Key generation phase, Pseudonym generation, Secret key generation phase and message authentication phase.

The proposed work employs blockchain technology to store the details of the incoming vehicles so that the vehicles will be authenticated based on the hash value generated using the vehicle identities (P_{ID}, C_{ID}, E_{ID}). The blockchain technology is composed of series of block registers that stores these hash values which assists in authentication process. In addition to the blockchain technology, the proposed work employs fuzzy logic to assist in determining the shortest path for the data communication between the OBU, MCU and TA. The fuzzy logic performs the detection of optimal path for data communication based on the fuzzy rule set.

The purpose of using block chain is to secure the data related to the incoming vehicles. Hence the data were stored in the form of hash values in the blockchain registry. These data are decentralized in nature and is maintained by the Trusted Authority (TA) of the smart city. The reward of incorporating the blockchain technology in the proposed work enhances the level of security, such that after the successful validation of authentication process, a Ticket has been generated to the incoming vehicle. The vehicle traveling without ticket will be considered as Unauthorized vehicle and will not be permitted to enter the city. The Proof of Presence (PoP) is the name of the consensus theorem employed in the proposed work.

3.2.1 Initialization phase

The Trusting Authority (TA) validates the OBU by employing the Elliptic Curve Cryptography (ECC) as illustrated in this initialization phase. In the initialization phase, the trusted authority is the only agent involved in the process, generates the necessary hash functions, creates a own private key from which the public key is generated. In addition, the TA produce a random key which is kept secret, for the initialization process as described below.

Algorithm for initialization phase:

i. Consider any random prime numbers 'p' and 'q' to employ $y^2 = x^3 + px + q$ mod q while P is the generator of the non-cyclic group G.

ii. Select public keys (PU_{TA}) of the TA at random and compute private key using $Pr_{(TA)} = q * PU_{(TA)} * G$.

iii. Generate three way hash functions h_1, h_2 and h_3 as defined in following equations:
$h_1 \rightarrow (0,1) * G_1$;
$h_2 \rightarrow (0,1) * G_1 * G_2$
$h_3 \rightarrow (0,1) * G_1 * G_2 * G_3$
Where, G_1, G_2, and G_3 are the non-cyclic groups generated by the Elliptic Curve Cryptography.

iv. Choose a random key rk_i and determine $\rho_i = h_1(rk_i||P_{ID}||C_{ID}||E_{ID})$ where P_{ID}, C_{ID}, E_{ID} are the number place identity, chase identity and engine identity respectively.

v. The TA, maintains the secrecy of the rk_i and generates initialization ticket TKT_i and publishes the system parameters,

$$p = (h_1, h_2, h_3, p, q, PU_{TA}).$$

The trusted authority (TA) generates the hash values, public key and private keys along with the secret random key. Keeping the random key secretly, the hash values and public keys are published to make available to the vehicles. The hash functions play a vital role in the proposed blockchain based vehicular communication system. The chain of contents communicated by the vehicles (OBU)was stored in the blockchain registry in the form of chain. The hash function performed in the proposed work is illustrated in Figure 3. The Proof of Presence (PoP) is described in the Figure 2, where, the transaction 1(communication of the vehicle identity to the authentication server)by the OBU is identified by the hash value using (P, h_n), where P represents the path and here in transaction 8, the 'P' value represents the L, L, L, R.

The binary tree in Lexicographical Merkle Tree (LMT), performs the validation of the single node with two pairs of strings namely (C,H)and (C*, H*). The blockchain C will be present in the left side only if $C < C*$, else the block B will be placed on the right side of C*. The proof of Presence is depicted in Figure 3. In the Figure 3, the proof of Presence is validated by two adjacent credentials (C, C*) in the Lexicographical Merkle Tree (LMT).

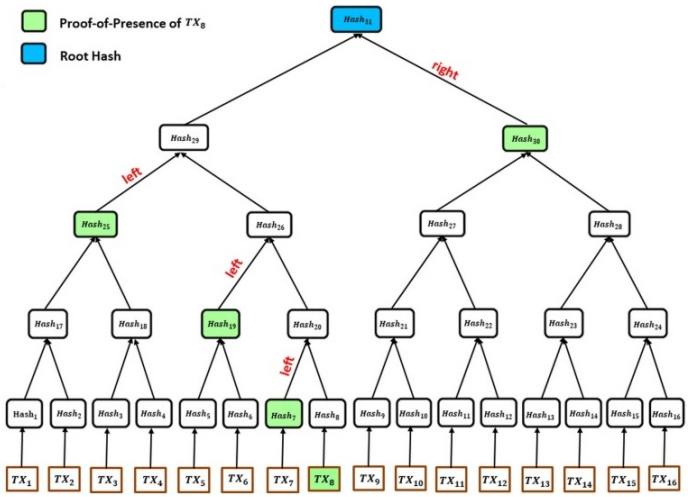


Figure 3: Hash function representing the Proof of Presence

In the Figure 4, the proof of absence is validated by two adjacent credentials (H, H*) in the Lexicographical Merkle Tree (LMT). The proof of absence is depicted with an example of considering two adjacent credentials (C_9, C_{10}). To validate the blockchain C_9 and C_{10}, proof of absence is considered by including the blockchain C_8 and C_{15}. This process will assist the proposed work during the validation process, thus decides whether the incoming vehicle (OBU) is an existing or a new one.

3.2.2 Key generation phase

In the secret key generation phase, the incoming new vehicle register itself with its identity namely the number plate identity (P_{ID}), Chase identity (C_{ID}) and the engine identity (E_{ID}) with the TA to perform the registration process and to receive the secret token for registration (TKT_i) from the TA. The step by step process involved in the secret

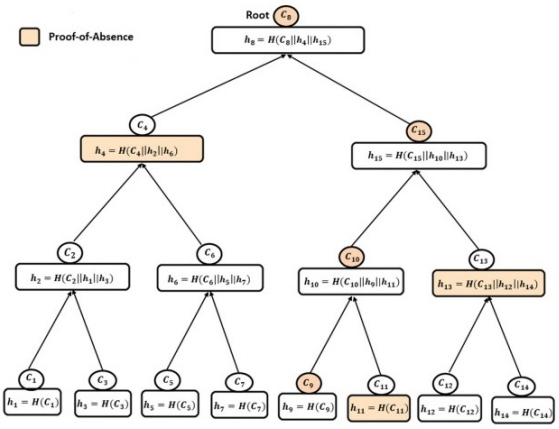


Figure 4: Proof of Absence using Lexicographical Merkle Tree (LMT)

key generation phase by the OBU (vehicle) is illustrated.

Algorithm for key generation phase:.
Input: Vehicle (V_i) identities.
Output: Registration confirmation R_c.

i. V_i computes, TKT_i=$h_1(PU_{TA}||(\rho_i)||P_{ID}||C_{ID}||E_{ID})$.

ii. **if** $(TKT_i^* == TKT_i)$.

iii. Return 'registration success'.

iv. Choose $h_{o,i}$ in random and compute $h_{1,i} = h_1(h_{0,i})$ // generation of hash chain.

v. Generate a random private key Pr_{Vi} and computes public key $PU_{Vi} = p * Pr_{Vi} * G$.

vi. Stores the hash chain code and registration ticket of membership $(h_{1,i}, TKT_i)$.

vii. Perform generation of temporary key (α_i, β_i).
$\alpha_i = K_i * \gamma_i * P$.
$\beta_i = K_i * \gamma_i * q + x$.
Where, p and q are the cyclic groups and K_i is the shared key while γ_i is the random number chosen.

viii. V_i furnishes the identity (P_{ID}, C_{ID}, E_{ID}) to TA and DRA through the channel in a secured manner and stores the temporary secret keys α_i, β_i.

ix. **Return** α_i, β_i.

x. else.

xi. **Return** "Trust Validation Failed".

xii. **End** Temporary Key Generation phase.

3.2.3 Pseudonym generation phase

The pseudonym generation phase is performed by the vehicle V_i to validate the status of the secret keys generated by the vehicle and to generate a pseudonym for each communication sessions. The process performed by the V_i is illustrated as follows.

Algorithm for Pseudonym generation phase:.
Input: Session ticket (TST_i).
Output: Pseudonym for the present session $(h_{n,i})$.

i. Compute $A_i = h_1(P_{ID}||par||PU_i)$ on reception of TST_i // Compute secret key and validates the validity of the ticket TST_i.

ii. $\beta_i = K_i + PU_i$ //// Determine the validity of the secret key.

iii. **If** $(\beta_i* == \beta_i)$, then.

iv. **Return** "Accept Secret Key".

v. **else** "Reject Secret Key".

vi. Generate pseudonym, $PN_i^k = h_2(P_{ID}||h_{n,i}||PU_I||T); n = 1, 2, 3, 4, \ldots....$

vii. $h_{(n,i)} = h_1 h_{(n-1),i}$.

viii. **Return** PN_i^k.

ix. **end if**.

x. **End** Pseudonym generation phase.

3.2.4 Secret key generation phase

The new vehicle on validating the status of the registration ticket and the key, tend to generate a pair of keys namely the secret key and the public key of the vehicle V_i. This process is considered as the initial process for communication between the OBU and the MCU. The process involved in the secret key generation phase is illustrated below.

Algorithm for secret key phase:.
Input: random number u_i.
Output: Secret key (SK_i) and Public key (PU_i).

i. Generate random number $u_i \epsilon G$.

ii. Compute public key $PU_i = u_i * P$.

iii. Compute secret key $SK_i = (u_i, \beta_i)$.

iv. **Publish** PU_i.

v. **End** Secret key generation phase.

In algorithm, the vehicle V_i i.e. the OBU generates its own private key which is considered as the secret key (SK_i) and a public key (PU_i) which will be published to the TA and the MCU.

3.2.5 Message authentication phase

On successful registration and the generation of the keys by the incoming vehicle, the V_i initiates its communication with the DRA through the cloud server. The message communicated from V_i to cloud server is a time stamped and requires proper authentication from the V_i to accept the incoming message. This message authentication phase involves the process of signing the message and to authenticate the message from the V_i. The processes involved in the message signing and authentication is illustrated below.

Algorithm for message authentication phase:
Input: Previous hash value.
Output: Signature (S_i) and Vehicle identity (v_{ID}).

i. Choose two random numbers r_x, $r_y \in G$ and compute $h_i^n = h_2(U_i||P_{ID}||\beta_i||PU_i)$.

ii. $C_i = r_1 h_1 + r_2^2 h_2^2$.

iii. Compute $h_i^{(n+1)} = h_3(U_i||P_{ID}||C_i||PN_i)$.

iv. If $h_i^{(n+1*)} = h_i^{(n+1)}$.

v. **Return** Message Validated.

vi. $v_i = r_1 h_1 + r_2^2 h_2^2 + U_i h_3^3 + \beta_i$ // Generation of identity component for signature.

vii. $S_i = (\beta_i, v_i)$ // Signature of OBU(V_i)

viii. $T_n^{pres} - T_n^{prev} \leq \Delta T$ // Determination of time stamp difference.

ix. On successful verification of signature and the time stamp of the received message, determines the hash value validity.
$h_n^3 = h_n(v_i||P_{ID}||PU_i||T_n^{Pres})$.

x. If $h_n^{3*} == h_n^3$.

xi. Compute $v_{ID} = V_i + h_n^3 PK_i + PU_i$.

xii. If $v_{ID}^* == v_{ID}$.

xiii. Compute $\sum_{i=1}^{m} v_i * U_i = \sum_{(i=1)}^{m} (v_i * h_3 * \beta_i) + PU_i$.

xiv. **Return** Accept request from V_i.

xv. End if.

xvi. End if.

xvii. End if.

xviii. **End** message authentication phase.

The message authentication process accepts the communication from the OBU V_i to the MCU. The MCU processes the information from the OBU and analyzes the location and mobility status of the OBU. The communication message between the OBU and the MCU is given priority based on the type of the message. The vehicle such as ambulance and other safety vehicles communicate the high priority messages, such that the path related information is provided to the corresponding OBU. The shortest path to reach the destination by the OBU is identified by the neuro fuzzy algorithm as described in the upcoming section.

3.3 Neuro fuzzy based route determination

Neuro-fuzzy systems possess the ability to aid in routing decisions within scenarios [28] involving imprecise or ever-changing elements. By studying patterns in network traffic and adjusting routing choices according to fuzzy principles like "high traffic," "low latency," and "secured," they acquire knowledge. The routing decisions made by the Neuro-fuzzy system are securely recorded on the blockchain, ensuring transparency and traceability. Consequently, an indelible log of how data packets were directed is generated. The blockchain platform could be harnessed for the purpose of storing and authenticating network status information such as congestion levels. This information could then be utilized by the Neuro-fuzzy system to enhance its routing determinations. The incoming vehicles/OBU (V_i), on successful execution of registration process, will request for the best route for navigation which is provided by the neuro-fuzzy logic systems. This system also assists in transmitting the data from the Vi to the MCU in a shortest path. The structure of the neuro fuzzy logic system for determining the shortest path for transit is depicted in Figure 5.

The neuro fuzzy system is a contextual neural network which has multiple levels, namely the input layer, output layer and the fuzzy rules assisting in making decisions by the system. The neural fuzzy layer is composed of five layers of feed forward network followed by the layer of fuzzy rules, performing the fuzzification process. The layer 4 performs the defuzzification process to produce the output in the layer 5. The layers 2,3 and 4 are considered as the hidden layer, as it will not be exposed to the users. The proposed neuro fuzzy system is fed with the training data stored in the cloud servers and is expressed in terms of fuzzy rules as the learning process. The proposed work, employs two factors in the neural fuzzy system, namely the size of the packet (P_S) and the time stamp (T_v) of the vehicle / OBU (V_i). The packet size of the OBU is to be reduced in size, such that the data will be communicated safer and with authentication. The time stamp of the message is considered to be more vital, as the expired message will not be considered for processing. In this proposed work, the Center of Sums (CoS) method of defuzzification process is employed, which determines the incoming fuzzy sets (weightage) of all vehicles and based on the fuzzy sets (weightage) of the vehicle the shortest path has been provided. In case of reporting a valid location of both sender (OBU) and the receiver (MCU), the time

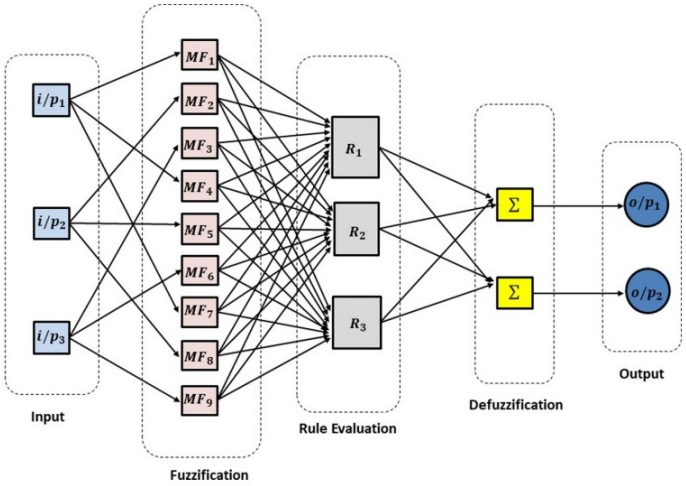


Figure 5: Neuro-Fuzzy Logic System for Shortest path determination

required for the time stamp shall be determined by measuring the distance between the OBU and MCU. It is assumed that the data packet is transferred at the velocity of light and it is considered that the OBU and MCU are at the line of sight. The anticipated time required for the data communication from OBU to MCU is determined using the following equation.

$$T_A = \frac{D_{OBU \to MCU}}{S} + d_T.$$

Where, T_A is the anticipated time for data transmission, $D_{OBU \to MCU}$ is the Euclidean distance between the OBU and the MCU and S represents the rate of data communication. The velocity of the data transmission resembles the velocity of light and d_T represents the delay in data transmission. The Euclidean distance between the OBU and the MCU shall be determined as represented in following equation.

$$D_{OBU \to MCU} = \sqrt{(x_{OBU} - x_{MSU})^2 + (y_{OBU} - y_{MSU})^2}.$$

Where,$x_{OBU}, x_{MSU}, y_{OBU}, y_{MSU}$ are the location coordinates of the OBU and MSU respectively. The neural fuzzy system accepts the distance and time to transit as input data and is processed by the fuzzification process. The fuzzy rules fed as the training input to the neural fuzzy system is illustrated in Table 1.

Rule #	Packet size (P_S)	Transit Time (T_V)	Security Level	Transit path
1	Low	Small	Good	Shortest
2	Low	Average	Good	Shortest
3	Low	High	Poor	Shortest
4	Average	Small	Good	Shortest
5	Average	Average	Good	Medium
6	Average	High	Poor	Longest
7	High	Small	Poor	Longest
8	High	Average	Good	Longest
9	High	High	Poor	Longest

Table 1: Fuzzification process rules

The fuzzy rules defined in the Table 1 define that if the packet size is high or the transit time is high leads to poor level of security. The neuro fuzzy structure is fed with the above fuzzy rules, based on the understanding, training data, the neuro fuzzy system, determines the level of security and the path to transit the data. The longest data is to be transmitted in a shortest path to overcome the excess time consumption during the data transmission. In case of poor level of security, the misbehaving node or anomaly node (vehicle) is detected using the pattern of data transmitted by the OBU. When an anomaly OBU is detected in the network, the detected OBU reports a anomaly message pattern communicated to the MSU. The MSU communicates this anomaly message to DRA, to perform

authentication validation process and to validate the time stamp of the node as illustrated in the previous sections. The DRA performs the dispute handling process, by verifying the number plate identity, chase identity, and engine identity. The DRA generates a hash value using the above mentioned identity (P_{ID}, C_{ID}, E_{ID}) to determine the genuinity of the incoming vehicle. The DRA employs message verification and batch verification process to estimate the genuine level of the incoming /misbehaved nodes. The DRA verifies the authentication of the OBU by determining the consistency of the node as defined in equations below.

$$v_i P = (r_1 h_1 + r_2^2 h_2^2 + \cdots + r_n^n h_n^n).$$

$$v_i P = R_n H_n + PU_i.$$

Where, the v_i is the vehicle identity, whereas the $r_1 h_1, r_2^2 h_2^2, r_n^n h_n^n$ are the randomly generated fuzzy values of the incoming vehicle and the term 'h' is the corresponding hash function. The term P is the generator of the cyclic group "G" and R_n is the cumulative sum of the random numbers $r_1, r_2, \ldots r_n$.The term PU defines the private identity of the vehicle.The batch verification process enables the DRA to validate the authenticity of the misbehaved node in the network as represented in following equation.

$$\sum_{(i=1)}^{n} v_i P = \sum_{(i=1)}^{n} v_i (r_1 h_1 + r_2^2 h_2^2 + \cdots + r_n^n h_n^n) P.$$

The accuracy of the misbehaved vehicle shall be identified based on the identity and the hash value created by the vi to prove the authenticity of the vehicle.

4 Security analysis

i. **When a malicious node enters the VANET, and compromises security**.
Let's consider a malicious vehicle tends to break the security of the proposed vehicular network. The malicious vehicle node cannot able to compromise the security of the vehicular network, as the incoming V_i needs to perform the registration process and to communicate the identities P_{ID}, C_{ID}, E_{ID} to the Trusted Authority (TA) for receiving the registration ticket (TKT_i). The identity of the malicious node will be determined based on the three identities and the ticket will not be issued. Hence the new malicious vehicle, shall not succeed the registration process and cannot compromises the VANET security.

ii. **Key compromise attack**.
Let's consider that the incoming malicious vehicle (V_i) tends to know the public key of the trusted authority and the authorized vehicle (V_i), compromise the identity of the genuine user by detecting the private key of the authorized vehicle. The private key of the vehicle (α_i, β_i) are generated by the authorized vehicle and is kept secret without disclosing to others. The vehicle employs the Elliptical Curve Cryptography to generate the pair of keys which makes hard to duplicate or guess the pair of private keys. Hence the proposed work proves robust against the key compromise attack.

iii. **Man-in-the-middle attack**.
The Man-in-the-Middle (MitM) attack is the critical attack, in which the attacker tends to break the message communication between the authenticated vehicle and the trusted party or the MCU. Let's consider that an attacker tends to position in between the OBU and the MCU or TA. In this case, the communication between the OBU and the MCU/TA is encrypted using the private key of the vehicle (α_i) and the private key of the TA which is known only to the corresponding parties. Hence it is tedious to break the communication pattern between the trusted parties thus proving robust against the MitM attack.

iv. **Vehicle forgery attack**.
Let's consider that a malicious vehicle forgeries its number plate identity and tends to be a genuine vehicle. In this case the malicious vehicle shall duplicate the number plate identity, whereas unable to perform duplicate in the engine and chase identity as it is fixed and unique to all vehicles. The identities P_{ID}, C_{ID}, E_{ID} cannot be duplicated completely, and is proved to robust against the vehicle forgery attack.
The proposed work is proved to be secure against most common attacks and the performance evaluation is performed in terms of packet delivery ratio, end to end delay,etc.

4.1 Packet delivery ratio (PDR)

The Packet delivery ratio is a metric of the network, which determines the rate of successful delivery of the data packet from source node (vehicle) to the destination node (MCU). The packet delivery ratio of the proposed work is compared with the conventional method of VANET and the results are depicted in Table 2. The formula for determining Packet Delivery Ratio is defined in following equation.

$$PDR = \frac{N_{P-BS}}{P_T}.$$

Where, N_{P-BS} is the number of packets reached the base station, while P_T is the total packets transmitted.

Packets #	K.Lakshminarayanan [17]	J.Qi[20]	Y.Huang[11]	M.K.Diaa[6]	Proposed Method
500	96.15	92.05	90.15	89.68	99.32
1000	95.96	91.15	89.99	88.59	99.18
1500	94.02	90.15	88.68	88.57	99.01
2000	92.12	88.57	86.24	87.54	98.65
2500	90.74	87.87	86.21	86.01	98.43
3000	89.98	86.04	86.08	85.76	98.11

Table 2: Comparison of Packet Delivery Ratio

Figure 6 illustrates that the proposed blockchain framework of VANET, apart from offering a better level of security to the communication, also offers a better packet delivery ratio with a maximum of 99.32% of packet delivery ratio between the OBU and MCU.

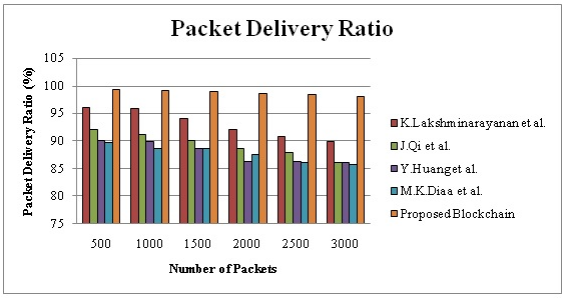


Figure 6: Comparison of Packet Delivery Ratio

4.2 End to end delay

The end to end delay is the time duration taken by the message packet to get transferred from source end to the destination end. The proposed work employs the encryption scheme and transfers the data in the encrypted format and hence it is necessary to measure the end to end delay of the data transmission. Table 3 defines the end to end delay of the proposed work and is compared with the state of art methodologies in VANET data communication

Packets #	K.Lakshminarayanan [17]	J.Qi[20]	Y.Huang[11]	M.K.Diaa[6]	Proposed Method
500	23.13	25.12	26.27	27.12	21.01
1000	24.15	26.27	28.24	29.15	22.65
1500	25.95	27.56	28.98	29.75	22.92
2000	26.64	28.45	28.99	30.24	24.02
2500	27.01	29.65	30.65	31.58	25.85
3000	30.68	31.25	32.45	33.01	27.10

Table 3: Comparison of End to End Delay

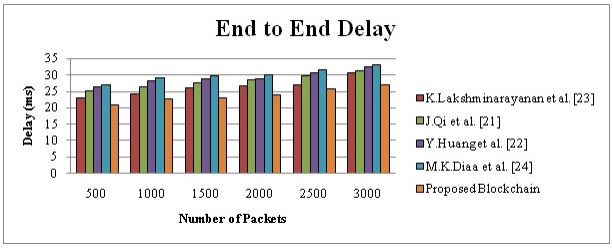


Figure 7: Comparison of end to end delay

The Figure 7 depicts the comparative analysis of the end to end delay experienced by the proposed work and is compared with the state of art methodologies. The proposed work experiences a reduced end to end delay when compared to the other works. The proposed work possesses the blockchain as the major technology in this domain, and is employed for performing security validations of the incoming vehicles. However, the blockchain technology itself possesses a major concern of scalability and potential latency. Despite the performance challenge, this proposed work overcomes the challenge of potential latency through the integration of blockchain and neuro fuzzy logic. The neuro fuzzy logic assists the blockchain in terms of data validations and the scalability issues have been overcome through the fuzzy rules.

4.3 Communication overhead

The communication from one OBU to another OBU or to the TMC unit necessitates the inclusion of source and destination address along with the routing information. This consumes larger communication overhead, which in turn consumes huge processing time. The excessive processing time creates delay in the data transmission, which directly influences the end-to-end propagation delay. The communication overhead is minimized in the proposed work, as it holds the information related to the source and the destinations shown in Table 4. The routing policy followed here is the dynamic routing policy which was influenced by the neighboring routers.

Comm. Overhead #	K.Lakshminarayanan [17]	J.Qi[20]	Y.Huang[11]	M.K.Diaa[6]	Proposed Method
Bytes	1026	1024	1026	512	256

Table 4: Comparison of End to End Delay

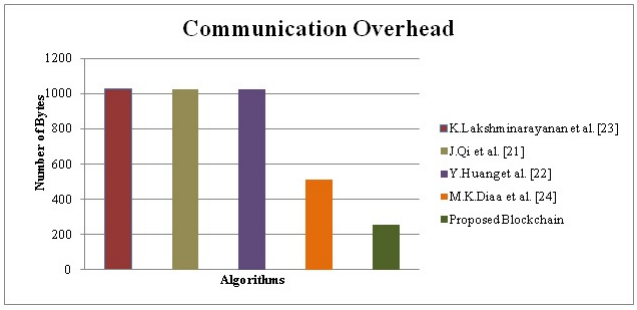


Figure 8: Comparison of communication overhead

Due to the possession of reduced communication overhead, the processing and the propagation delay has been mitigated to a greater extent. The graphical representation of comparing the performance of existing and proposed work in terms of communication overhead is illustrated in Figure 8.

4.4 Throughput

The term throughput defines the efficiency of the data communication. The proposed work is intended to communicate its identity and to receive the path based information from the TMC. The data communication between any two nodes

requires a better level of throughput. In this objective, the proposed work is analyzed in terms of throughput with a set of variable packet length over the designed network. The observed values are listed in the Table 5.

Packets #	K.Lakshminarayanan [17]	J.Qi[20]	Y.Huang[11]	M.K.Diaa[6]	Proposed Method
500	86.16	87.59	91.04	92.35	95.2
1000	85.15	86.15	90.22	91.25	95
1500	84.96	85.95	89.15	90.01	94.15
2000	83.12	84.85	88.15	89.15	93.65
2500	82.84	83.33	86.03	88.78	92.15
3000	80.01	82.18	85.41	86.15	91.85

Table 5: Comparison of throughput

The proposed work exhibits a better level of throughput when compared with the existing state of art methodologies. The proposed work exhibits a throughput of 95.2%, 95%, 94.15%, 93.65%, 92.15% and 91.85% for 500, 1000,1500,2000,2500 and 3000 packets respectively which is shown in Figure 9.

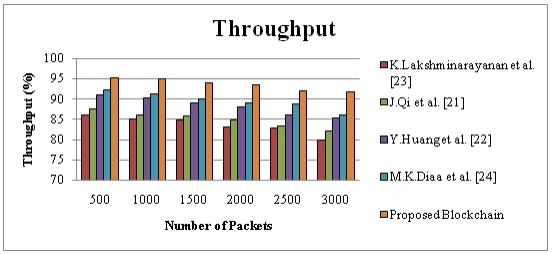


Figure 9: Comparison of throughput

4.5 Accuracy

The accuracy [1] is the term associated with the merit of predicting the anticipated parameters. The proposed work is intended to identify and to have a proper bifurcation between the new and the existing OBU. In this regard, the proposed work employs blockchain [4] so that to identify the new and existing OBU based on the hash code functions stored in the blockchain registry. The level of accuracy observed in the non-blockchain methods [5] and the proposed blockchain method is listed in Table 6.The term accuracy is determined in terms of True Positive (TP) and True Negative (TN). The term True positive refers to the perfect diagnosis [29] of matching between the incoming hash value and the previous hash value, while the True Negative is the correct prediction of mismatched hash values.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}.$$

The equation illustrates the method of determining the accuracy level [16], in which the False Positive (FP) refers to the wrong prediction of given hash value does not exists but actually it exists. Similarly the False Negative (FN) refers to the wrong prediction of given hash value matches but actually it does not exist.

Packets #	K.Lakshminarayanan [17]	J.Qi[20]	Y.Huang[11]	M.K.Diaa[6]	Proposed Method
500	75.58	78.95	79.91	81.25	91.05
1000	74.15	77.58	78.14	80.56	89.16
1500	72.69	76.35	76.25	80.16	88.65
2000	71.58	75.14	75.85	79.52	87.31
2500	70.69	73.03	72.15	78.03	86.01
3000	65.25	70.15	70.02	77.71	86

Table 6: Comparison of accuracy

The proposed work experiences a better level of accuracy when compared to the existing works, which were employing methodologies other than blockchain technique represented in Figure 10. The maximum accuracy exhibited by the proposed work is 91.05% which is better than the existing works.

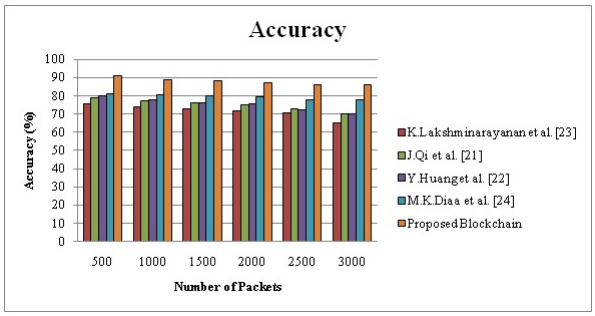


Figure 10: Comparison of Accuracy

5 Conclusion

In recent years, the technology plays a vital role in modernizing the human environment with advanced automation technology. One such application is the smart city which employs the vehicular network (VANET) enabling the vehicles to communicate with each other and with the Mobile Control Unit (MCU). This communication among the vehicles enables the vehicles to select a best path and to move faster to the destination. The communication in the VANET is highly prone to the security, as the data is exposed to the malicious insiders of the network. To overcome this challenge, the proposed work is introduced with the blockchain technology to enhance the level of security. The proposed work employed blockchain technology along with the neural fuzzy logic for the routing process. The security analysis of the proposed work proves to be secured against malicious attacks and the performance analysis proves that it stays superior in terms of packet delivery ratio and end to end delay. The proposed work outperforms the existing works with 98.11% of packet delivery ratio, 27.10% of end to end delay due to the employment of 256 bytes of communication overhead. In addition, the proposed work experiences a better throughput with 91.85% and accuracy of 86% for 3000 number of input packets. The major practical implementation consideration experienced in the proposed research work is the enhancement of latency in authentication process due to the increase in volume of the hash records (chain) in the blockchain technology. This potential hindrance shall be overcome by incorporating an optimization algorithm to identify the genuine (frequent) users during authentication process.The performance and the security of the proposed work shall further be enhanced in the future, through the incorporation of the Artificial Intelligence Technique for the performance enhancement. The security of the proposed work shall further be enhanced by performing key generation using novel and secure algorithms, such that the level of robustness shall be enhanced.

Acknowledgement

The authors wish to express their appreciation for several excellent suggestions for improvements in this paper made by the referees.

References

[1] N. Aishwarya, N. G. Praveena, C. Karthikeyan, S. Priyanka, *IoT enabled detection and notification system for potholes and road cracks*, Disruptive Technologies for Big Data and Cloud Applications. Lecture Notes in Electrical Engineering, **905** (2022), 799-806. https://link.springer.com/chapter/10.1007/978-981-19-2177-3_74

[2] A. Bhatia, K. Haribabu, K. Gupta, A. Sahu, *Realization of flexible and scalable VANETs through SDN and virtualization*, International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, (2018), 280-282. https://doi.org/10.1109/ICOIN.2018.8343125

[3] C. Chen, L. Liu, T. Qiu, D. O. Wu, Z. Ren, *Delay-aware grid-based geographic routing in urban VANETs: A backbone approach*, IEEE/ACM Transactions on Networking, **27**(6) (2019), 2324-2337. https://doi.org/10.1109/TNET.2019.2944595

[4] M. Deveci, I. Gokasar, D. Pamucar, A. Alaa Zaidan, X. Wen, B. B. Gupta, *Evaluation of cooperative intelligent transportation system scenarios for resilience in transportation using type-2 neutrosophic fuzzy VIKOR*, Transportation Research Part A: Policy and Practice, **173** (2023), 103666. https://doi.org/10.1016/j.tra.2023.103666

[5] M. Deveci, D. Pamucar, I. Gokasar, M. Köppen, B. B. Gupta, *Personal mobility in metaverse with autonomous vehicles using Q-rung orthopair fuzzy sets based OPA-RAFSI model*, IEEE Transactions on Intelligent Transportation Systems, **24**(12) (2023), 15642-15651. https://doi.org/10.1109/TITS.2022.3186294

[6] M. K. Diaa, I. S. Mohamed, M. A. Hassan, *OPBRP- obstacle prediction based routing protocol in VANETs*, Ain Shams Engineering Journal, **14**(7) (2023), 101989. https://doi.org/10.1016/j.asej.2022.101989

[7] X. Guo, Y. Chen, L. Cao, D. Zhang, Y. Jiang, *A receiver-forwarding decision scheme based on Bayesian for NDN-VANET*, China Communications, **17**(8) (2020), 106-120. https://doi.org/10.23919/JCC.2020.08.009

[8] M. Hashem Eiza, T. Owens, Q. Ni, *Secure and robust multi-constrained QoS aware routing algorithm for VANETs*, IEEE Transactions on Dependable and Secure Computing, **13**(1) (2016), 32-45. https://doi.org/10.1109/TDSC.2014.2382602

[9] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan, A. Aldegheishem, *Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles*, IEEE Access, **8** (2020), 199618-199628. https://doi.org/10.1109/ACCESS.2020.3034327

[10] S. Hu, Y. Jia, C. She, *Performance analysis of VANET routing protocols and implementation of a VANET terminal*, 2017. International Conference on Computer Technology, Electronics and Communication (ICCTEC), Dalian, China, (2017), 1248-1252. https://doi.org/10.1109/ICCTEC.2017.00272

[11] Y. Huang, M. Ma, *ILL-IDS: An incremental lifetime learning IDS for VANETs*, Computers and Security, **124** (2023), 102992. https://doi.org/10.1016/j.cose.2022.102992

[12] R. Hussain, F. Abbas, J. Son, H. Eun, H. Oh, *Privacy-aware route tracing and revocation games in VANET-based clouds*, 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Lyon, France, (2013), 730-735. https://doi.org/10.1109/WiMOB.2013.6673437

[13] R. Hussain, J. Son, H. Eun, S. Kim, H. Oh, *Rethinking vehicular communications: Merging VANET with cloud computing*, 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings, Taipei, Taiwan, (2012), 606-609. https://doi.org/10.1109/CloudCom.2012.6427481

[14] K. Kandali, L. Bennis, H. Bennis, *A new hybrid routing protocol using a modified K-means clustering algorithm and continuous hopfield network for VANET*, IEEE Access, **9** (2021), 47169-47183. https://doi.org/10.1109/ACCESS.2021.3068074

[15] R. Kaur, T. P. Singh, V. Khajuria, *Security issues in vehicular Ad-Hoc network (VANET)*, 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, (2018), 884-889. https://doi.org/10.1109/ICOEI.2018.8553852

[16] P. S. Kumar, *Computationally simple and efficient method for solving real-life mixed intuitionistic fuzzy 3D assignment problems*, International Journal of Software Science and Computational Intelligence, **14**(1) (2022), 1-42. https://doi.org/10.4018/ijssci.291715

[17] K. Lakshmi Narayanan, R. Naresh, *An efficient key validation mechanism with VANET in real time cloud monitoring metrics to enhance cloud storage and security*, Sustainable Energy Technologies and Assessments, **56** (2023), 102970. https://doi.org/10.1016/j.seta.2022.102970

[18] Z. Onder, E. Savas, I. Canak, *Some novel approaches on the* $(\overline{N}, p, q)$ *summability of double sequences of fuzzy numbers and its applications*, Iranian Journal of Fuzzy Systems, **20**(6) (2023), 105-122. https://doi.org/10.22111/ijfs.2023.44900.7922

[19] D. Prabakaran, H. Sathyapriya, *A review on methodologies and performance analysis of device identity masking techniques*, International Journal of Scientific and Technical Research, **8**(12) (2019), 2018-2022. https://www.ijstr.org/final-print/dec2019/A-Review-On-Methodologies-And-Performance-Analysis-Of-Device-Identity-Masking-Techniques.pdf

[20] J. Qi, T. Gao, C. Zhao, *A pseudonym based certificateless privacy preserving authentication scheme for VANETs*, Vehicular Communications, **38** (2022), 100535. https://doi.org/10.1016/j.vehcom.2022.100535

[21] M. Sayad Haghighi, Z. Aziminejad, *Highly anonymous mobility-tolerant location-based onion routing for VANETs*, IEEE Internet of Things Journal, **7**(4) (2020), 2582-2590. https://doi.org/10.1109/JIOT.2019.2948315

[22] J. Shen, C. Wang, A. Castiglione, D. Liu, C. Esposito, *Trustworthiness evaluation-based routing protocol for incompletely predictable vehicular Ad Hoc networks*, IEEE Transactions on Big Data, **8**(1) (2022), 48-59. https://doi.org/10.1109/TBDATA.2017.2710347

[23] G. D. Singh, M. Prateek, S. Kumar, M. Verma, D. Singh, H. N. Lee, *Hybrid genetic firefly algorithm-based routing protocol for VANETs*, IEEE Access, **10** (2022), 9142-9151. https://doi.org/10.1109/ACCESS.2022.3142811

[24] M. Syfullah, J. M. Y. Lim, *Data broadcasting on cloud-VANET for IEEE 802.11p and LTE hybrid VANET architectures*, 3rd International Conference on Computational Intelligence and Communication Technology (CICT), Ghaziabad, India, (2017), 1-6. https://doi.org/10.1109/CIACT.2017.7977321

[25] A. M. R. Tolba, *Trust-based distributed authentication method for collision attack avoidance in VANETs*, IEEE Access, **6** (2018), 62747-62755. https://doi.org/10.1109/ACCESS.2018.2875906

[26] P. Upadhyay, V. Marriboina, S. Kumar, S. Kumar, M. A. Shah, *An enhanced hybrid glowworm swarm optimization algorithm for traffic-aware vehicular networks*, IEEE Access, **10** (2022), 110136-110148. https://doi.org/10.1109/ACCESS.2022.3211653

[27] Y. Wang, X. Li, X. Zhang, X. Liu, J. Weng, *ARPLR: An all-round and highly privacy-preserving location-based routing scheme for VANETs*, IEEE Transactions on Intelligent Transportation Systems, **23**(9) (2022), 16558-16575. https://doi.org/10.1109/TITS.2021.3134686

[28] Z. L. Yue, C. Yue, X. H. Peng, W. Wu, *VIKOR-based group decision-making method for software quality assessment*, Iranian Journal of Fuzzy Systems, **20**(1) (2023), 53-70. https://doi.org/10.22111/ijfs.2023.7346

[29] A. P. Zabaleta, P. Fernández, J. F. Prados-Castillo, M. de Castro-Pardo, *Constructing fuzzy composite indicators to support water policy entrepreneurship*, Sustainable Technology and Entrepreneurship, **1**(3) (2022), 100022. https://doi.org/10.1016/j.stae.2022.100022

[30] S. S. Zalte, V. R. Ghorpade, R. K. Kamat, *Synergizing blockchain, IoT, and AI with VANET for intelligent transport solutions*, Emerging Computing Paradigms: Principles, Advances and Applications, Wiley, (2022), 193-210. https://doi.org/10.1002/9781119813439.ch11

[31] J. Zhang, J. Wei, *On the security of privacy-enhanced authentication protocol for federated learning in VANETs*, IEEE Transactions on Information Forensics and Security, **19** (2024), 9433-9435. https://doi.org/10.1109/TIFS.2024.3445730