ISSN: 0067-2904

Fuzzy Logic-Based Authentication Protocol for VANETs Networks

Israa Nasir Abdulhussien*
Deparment of Computer Science, College of Science, Kufa University, Qadissiya, Iraq

Received: 11/10/2024 Accepted: 10/3/2025 Published: 30/3/2026

Abstract

The development of trust between vehicles in vehicular ad hoc networks (VANETs) serves as a fundamental requirement to guarantee application integrity while maintaining dependability. Reliability and trust allows vehicles to retrieve precise and dependable data from adjacent vehicles to perform the necessary decisions. Security remains difficult in VANET because it lacks central control and is characterized by dynamic operation methods. The main objective centers on developing more effective message verification systems. Since trust exists as a fuzzy concept, we implemented fuzzy logic to obtain trust values. The proposed system divides its functionality into two components which include a controller check stage built with four factors. Four factors establish the validity and legitimacy of vehicles in successful verification processes. Following the initial stage, the four factors proceed to the fuzzy system, allowing it to handle imprecise information and environmental uncertainties that exist during vehicle dynamics.

Keywords: fuzzy logic; protocol; network; authentication; VANET.

بروتوكول المصادقة القائم على المنطق الضبابي لشبكات *VANETs*

اسراء ناصر عبدالحسين

علوم الحاسبات، علوم الحاسبات، جامعة الكوفة، القادسية، العراق

الخلاصة

إن تطوير الثقة بين المركبات في شبكات المركبات المخصصة (VANETs) يعد متطلبًا أساسيًا لضمان سلامة التطبيق مع الحفاظ على الموثوقية. تسمح الموثوقية جنبًا إلى جنب مع الثقة للمركبات باسترداد بيانات دقيقة وموثوقة من المركبات المجاورة لأداء القرارات اللازمة. يظل الأمان صعبًا في شبكات المركبات المخصصة (VANETs) لأنها تفتقر إلى التحكم المركزي وتتميز بطرق تشغيل ديناميكية. يركز الهدف الرئيس على تطوير أنظمة التحقق من الرسائل الأكثر فعالية. نظرًا لوجود الثقة بوصفها مفهوما غامضا، فقد قمنا بتنفيذ المنطق الضبابي للحصول على قيم الثقة. يقسم النظام المقترح وظائفه على مكونين يتضمنان مرحلة فحص وحدة التحكم المبنية على أربعة عوامل. تحدد العوامل الأربعة صحة وشرعية المركبات في عمليات التحقق الناجحة بعد المرحلة الأولية، تنتقل العوامل الأربعة إلى النظام الضبابي مما يسمح له بالتعامل مع المعلومات غير الدقيقة وعدم اليقين البيئي الذي يوجد أثناء ديناميكيات المركبة.

*Email : ijmm2010@gmail.com

.1. Introduction

Vehicle ad hoc networks (VANETs) are categorized as mobile ad hoc network (MANET) applications that may enhance traveler comfort and safety on the road. [1]-[2]. It is expected to make a wide range of communication-based automotive applications possible, such as various infotainment systems inside cars and services related to road safety [3]. Researchers focused on developing the vehicle and how to communicate with other vehicles and infrastructure to enable the vehicle to interact with its surroundings [4]. Traffic control, entertainment, safety applications, driving assistance, collision avoidance, and safety services are just a few of the services that VANET can provide. Nonetheless, VANET developers prioritized the delivery of crucial safety-related information [5] due to traffic issues that could be fatal and significantly delay travelers [6]-[7]-[8].

A fuzzy logic is a technique for understanding, measuring, and handling unclear, ambiguous, and uncertain attributes [9]-[10]. Fuzzy logic is not like classical logical systems in that it attempts to simulate the imprecise modes of reasoning that are vital to the remarkable human capacity to reason in an imprecise and uncertain environment [11]. The performance and flexibility of vehicular communication systems can be improved by utilizing fuzzy logic in VANETs to improve the network's performance and functionality[12].

Fuzzy logic models and expresses knowledge naturally and intuitively using linguistic variables and fuzzy rules. Labels like "high," "low," or "medium" that denote nebulous or subjective concepts are known as linguistic variables [13]- [14]. Fuzzy operators like AND, OR, and NOT combine many antecedents in fuzzy rule sets[15]. Typically, linguistic variables are organized into three parts: a rule basis, a term set, and a name. The labels of linguistic values make up the term set, and the rule base establishes the connections between those terms[16]. Usually, these rules are written in an "if-then" structure, with fuzzy conditions in the antecedent (if-part) and fuzzy actions or conclusions in the consequent (then-part) [17]. Fuzzy data must also be translated from crisp data in both the input and the output. All of these tasks are completed by fuzzification, the first phase[18] .

The second stage involves starting the fuzzy inference process by combining the control rules and Membership Functions to produce the control output[19], which is then arranged into a table known as the lookup table. The fuzzy inference process revolves around the control rule[20], which has a direct bearing on human intuition and feeling also in VANET networks [21].

Based on the current input, a control output from the lookup table created in the previous phase should be chosen during an actual application. Moreover, the control operator should get that control output once it has been transformed back from the linguistic variable to the crisp variable. We refer to this procedure as step 3 or defuzzification [22].

Fuzzy Numbers of Restricted Shape can represent the gradual change in membership degrees in a linear, triangular, trapezoidal, Gaussian, or other shape[23]-[24].

The contributions of this work can be summarized as follows:

o New Fuzzy Logic-Based Authentication Framework: We establish a fuzzy logic-based framework that assesses multiple attributes to determine the trustworthiness of a vehicle handler.

o Enhanced Security: The protocol is resistant to several security threats.

o Contextual Parameter integration: Instead, the real parameters, such as timestamps, node ID, position, and vehicle behavior, are included in the protocol.

The next section includes a literature survey, a brief discussion of the method and the underlying rationale for using it; each module will then be described and discussed in detail.

Since fuzzy logic is the primary methodology used in this study, our proposal was efficacy, not obvious, and needs no user intervention.

2. literature survey

R. Kait et al. (2024) suggested that a trusted routing protocol for vehicle cloud networks establishes the safest route for data distribution to choose or reject a path, and Fuzzy Logic evaluates the node candidacy. This study determined a secure path based on trust in addition to variables like speed, proximity to other nodes, signal strength, and separation from nearby nodes. Simulations show that Fuzzy logic-based Trusted Routing Protocol maintains a high packet delivery ratio with minimal overhead and low delay, making it a promising solution for deploying Vehicular Cloud Networks in smart cities using electric vehicle technologies[25].

M. Gayathri and C. Gomathy (2023) proposed a solution to the black hole attack, which is a major issue in VANET, aiming to hack the entire communication network by dropping transmitted packets or introducing itself as a node with the shortest path. To prevent communication with attacked nodes, a Trust-Based Authentication Scheme is used, with Fuzzy Authentication to provide Trust-Based Security[26].

M. M. Hasan et al. (2023) suggested a new approach to model malicious vehicle properties using fuzzy sets, content tampering impact, and an inter-edge trust transfer mechanism. Compared to existing schemes, it outperforms with higher recall, precision, and accuracy and reduces end-to-end delay and messages per data packet[27].

P. Patankar et al. (2024) proposed to optimize traffic flow at intersections or merge points by considering real-time traffic density, vehicle speed, and queue length. It helps vehicles make decisions about speed adjustment, lane change, or breaking to avoid collisions. Fuzzy logic AI technology in VANETs can help balance travel time, fuel efficiency, and safety[28].

3. Proposed Security System

Vehicular Ad Hoc Networks (VANETs) play a vital role in Intelligent Transportation Systems (ITS). Before tackling the security challenges in VANETs, it is essential to first establish the fundamental requirements necessary for the proper functioning of the network. Neglecting any of these requirements could result in potential security vulnerabilities. The key requirements include authentication, integrity, confidentiality, non-repudiation, availability, access control, real-time constraints, and privacy protection. Most of these requirements align with general security concerns in networked systems.

A secure communication channel and vehicle authentication are the goals of the proposed authentication protocol, which comprises multiple essential elements. Vehicle trustworthiness is assessed using fuzzy logic based on four pasts, timestamps, ID of the node, location, and vehicle behavior. The objective of this approach is to improve vehicle authentication in VANETs in terms of accuracy and reliability. It consists of two main steps: controller check and fuzzy logic.

3.1 Controller check

The four components of the recommended process begin with the startup phase, where each vehicle generates a digital certificate or unique identity that is securely kept. The timestamp thus becomes crucial in the process of verification. Next, verify the ID of the node and the location. Lastly, confirm the behavior of the vehicle. These four variables will be independently tested, with the outcome being incorporated into the fuzzy logic. It is confirmed that the fuzzy logic rules and membership functions capture the uncertainty surrounding the component mentioned above.

3.1.1 Timestamps

The lifetime of the message is a significant concern in VANET because of the high dynamic behavior and consequent high mobility of the vehicles. Stated differently, in the context of vehicles, newer messages are considered more dependable than those that have expired. The lifespan is the amount of time that passes between the event message's expiration time and the current time[29] . The suggested approach first verifies the event message's lifetime to handle outdated or expired messages as redundant messages. Additionally, the predicted message threshold time (Time threshold) will be assessed based on the kind of immediate and expected messages in the vehicular environment. When there is little traffic, it should be set to a large value; when there is a lot of traffic, it should be set to a small value. The event message will be deleted if it is too old or has expired. If not, it will move on to the next phase for more verification (see algorithm 1).

Algorithm (1)

input =Msg, immediate time, expected time
output= true or false
Timediff= Calculate-Diff (immediate time, expected time)
threshold= ExtractTime (expected time)
if Timediff<threshold
Then
X=true
Else
X=false
end

3.1.2 ID of node

Power authentications can use external ways to supply legitimate and trustworthy evidence to identify attacks. Conventional law enforcement agencies may use one of these external techniques. Authentication guarantees that the sender of a message is accurately identified[30]. To determine if the sender of an event message is permitted or not, we employ ID authentication. Vehicles with ID authentication can uniquely identify the sender of a message. An automobile can join the network thanks to this authentication as well. After ID authentication is completed, avoid particular attacks.

3.1.3 Location of vehicle

To validate the sender's identity, attributes, and claimed location, ID authentication and location authentication were implemented within the suggested plan.

The following are some of the variables that affect the candidacy of vehicle:
1. System pre-registration: The vehicle (sender) needs to have previously registered with the HC. The fact that its ID (ID sender) is present in the HC database serves as evidence of this.
2. Seed value exchange: The HC and the vehicle must agree on a legitimate seed value. For safe communication, this shared seed serves as a cryptographic key or reference.
3-The fact that its ID (ID sender) is present in the HC identity of the vehicle: The HC must be able to authenticate and verify the vehicle's ID (ID sender). The candidacy fails if the HC is unable to confirm the sender's identity using the encrypted data that was received (ENC(ID sender, ID recipient)).
4-Accurate decryption and response: The car needs to accurately decrypt the HC-sent random number M and reply with h=DCR(M). The vehicle's candidacy is deemed illegitimate if the reaction does not correspond with the anticipated outcome.

Suppose every region has a head control (HC), and when two cars need to communicate, the vehicle (sender) sends the ENC (ID sender, ID receiver) to the HC. The Head Control (HC) is responsible for deciding the candidacy of the car. HC acts as the central authority in the system, determining if a vehicle is authorized to engage in communication or perform the authentication procedure. Then, using the seed value that is exchanged with the automobile and a random number M that is transmitted by the HC, the authenticator procedure starts. The seed can be dynamically derived from M, Seed= $H(K_{shared}||M)$, where H is a cryptographic hash function such as SHA-256, and K a pre-shared secret key.
The benefit of generating M is if there is no new random number for each session, an attacker may be able to intercept the original message and resend it later to trick the system. Using M ensures that each authentication attempt is unique. M is produced and sent to the vehicle via HC. Sending the ENC(M) allows HC to verify whether the information is authentic. The vehicle sends R to HC which R= DCR(M). Then, HC calculates the difference between the M and the R-value calculated from the vehicle. After that, it compares the outcome with threshold T, as in algorithm 2 and Figure 1 below:

Algorithm 2
input= (ENC (identifier sender (IDs), identifier receiver (IDr)))
output= true or false
choose (M) by HC
HC send ENC(M)
Vehicle calculate R=DCR(m) sending to HC
if M-R< T then
z=true
else
z=false
end

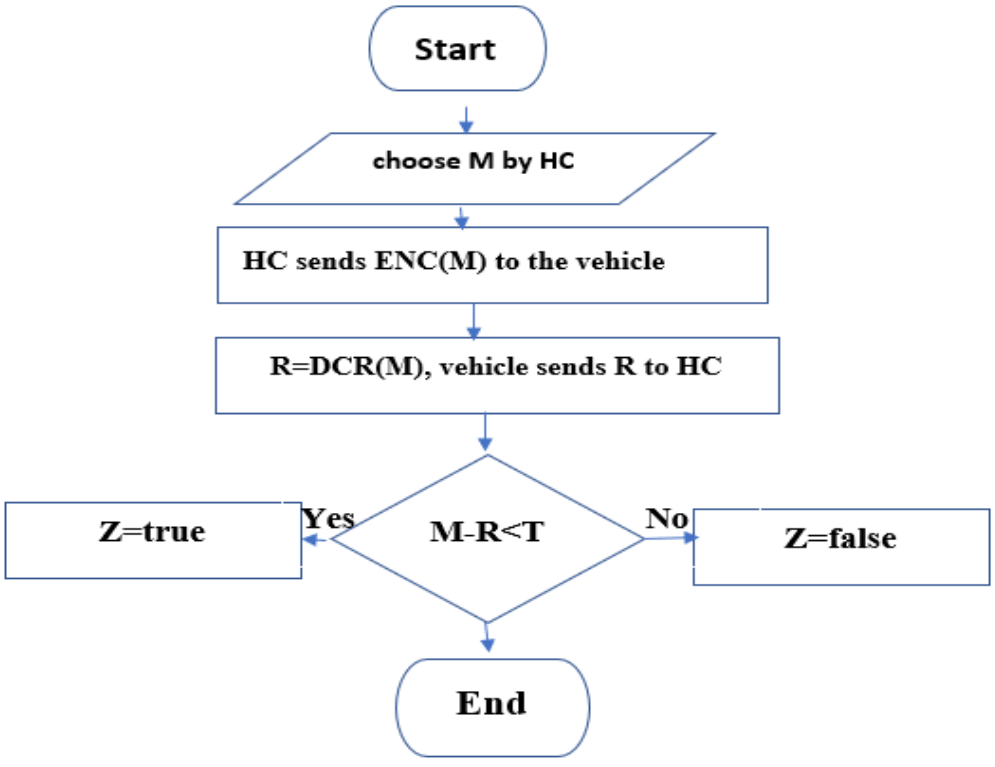

Figure 1: Location of vehicle

3.1.4 Vehicle behavior

We assume that there is a database containing the identifier of the infected vehicle by sending the vehicle ID and searching for it in the database. If it is not infected, it returns true, otherwise, it returns false, as in algorithm 3 below:

Algorithm 3

input =id of vehicle
output= true or false
Verify index table
If yes
Accepts the message
Z=true
Else
Discard message
Z=false
end

These four inputs (timestamps, ID of node, location of vehicle, vehicle behaviors) will move to the fuzzy logic section, through which we can know the reliability of this vehicle.

3.2 Authenticate by using fuzzy logic

A car sends a join request to nearby cars in an attempt to join the VANET. Calculating the distance between vehicles is very important in VANET systems, as it affects the reliability of the node requesting to join. The distance among the nearby cars is calculated using different methods such as GPS, RSSI,… etc. [31][32]. As prospective verifiers, the nearby cars apply fuzzy logic to determine how reliable the asking vehicle is. Fuzzy logic rules compute a trust level for the requesting vehicle based on the available data, including the node ID, timestamps, location, and vehicle behavior. The degree of trust indicates how likely it is that the car is real and reliable, as in algorithm 4 below:

Algorithm (4):

Input: Authenticate number, ID cluster, location, and vehicle behavior.
Output: AN=high or medium or low
A-Controller check
X=Timestamp
Y= ID cluster
Z= location
M= vehicle behavior
B-Authenticate by fuzzy logic
fuzzy algorithm (X, Y, Z, M)
β 1=X_i*α where α is the node's effect (high, medium, low)
β2=Y_i*α where α is the node's effect (high, medium, low)
β3=Z_i*α where α is the node's effect (high, medium, low)
β4=M_i*α where α is the node's effect (high, medium, low)

$$\beta = \sum_{j=1}^{4} \beta_j$$

$$\delta = \sum_{i=1}^{4} \alpha_i$$

$$€ = \frac{\beta}{\delta} * 100$$

T threshold = 0.7
if € > Threshold Then
Trust level=no hack

controller sends a message to the server that the vehicle is authenticated
Else
Trust level =hack
end
Periodic verification is an additional feature of the protocol that accounts for the dynamic nature of VANETs. Fuzzy logic is used to update car trust levels often in response to changing conditions and historical performance. Because of this, the protocol can adapt over time to consider cars whose dependability fluctuates.

3.2.1 Experience Measurement Module by Fuzzy Logic:

The vehicle's request to join is approved or denied based on the trust level determined using fuzzy logic. If the vehicle requesting access has a trust level greater than a predetermined threshold, access to the VANET is granted. If not, the request will be rejected, and the car won't be permitted admission.
The suggested authentication system, which uses fuzzy logic, provides a practical way to reduce security risks in VANETs. To evaluate the accuracy, efficiency, and resilience of the protocol against different attack scenarios, simulation-based assessments, and performance analyses are carried out. The outcomes show how the protocol can offer strong authentication and safe channels of communication, improving the general security and dependability of VANETs.
Time stamps, node IDs, location, and vehicle behavior all affect fuzzy routing. Figures 2, 3, 4, 5, and 6 define the four membership functions for linguistic variables. Moreover, Table 1 contains the fuzzy rules' specifications. When applying the weighted average approach, the result is crisp.

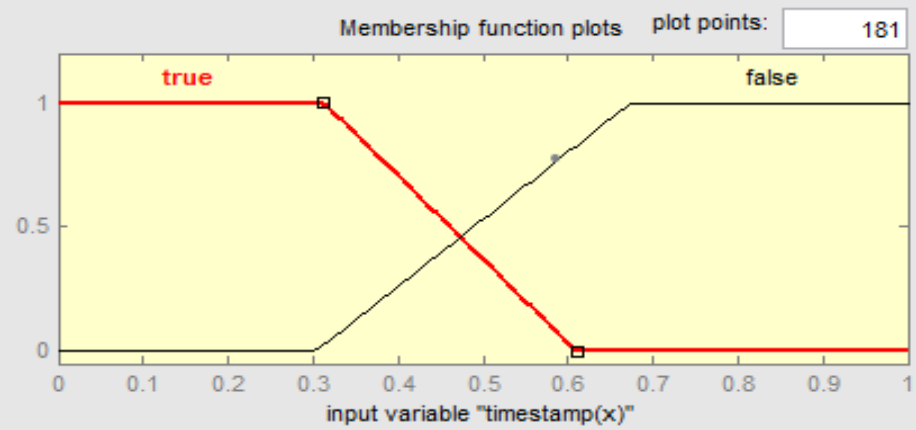

Figure 2: Timestamp level

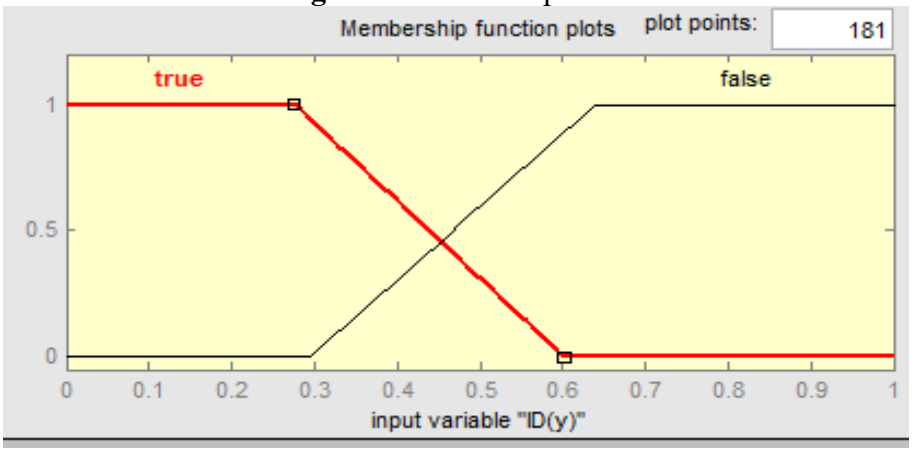

Figure 3: Node id level

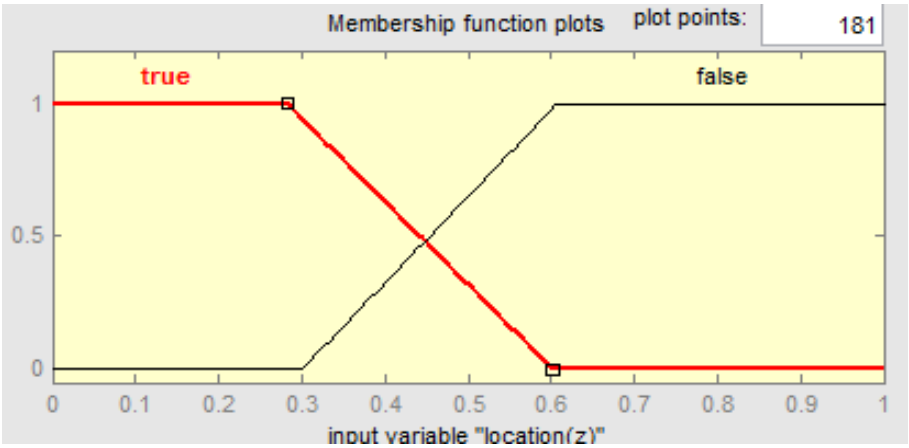

Figure 4: location level

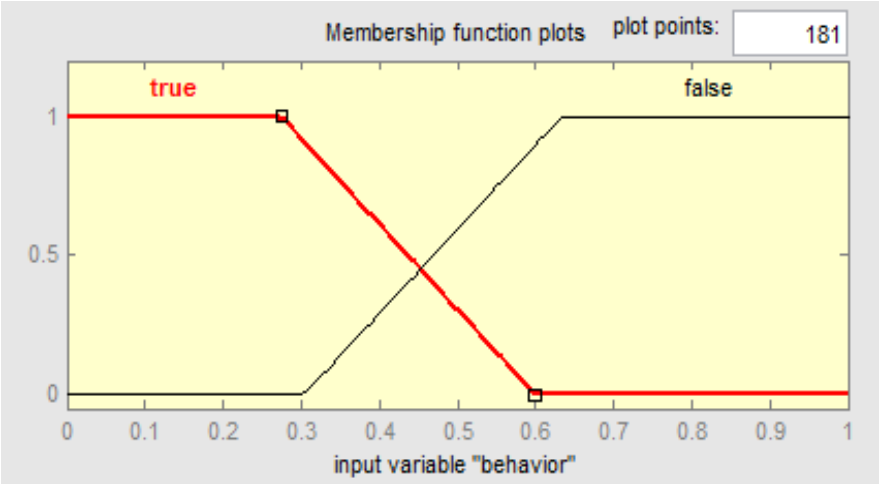

Figure 5: vehicle behavior level

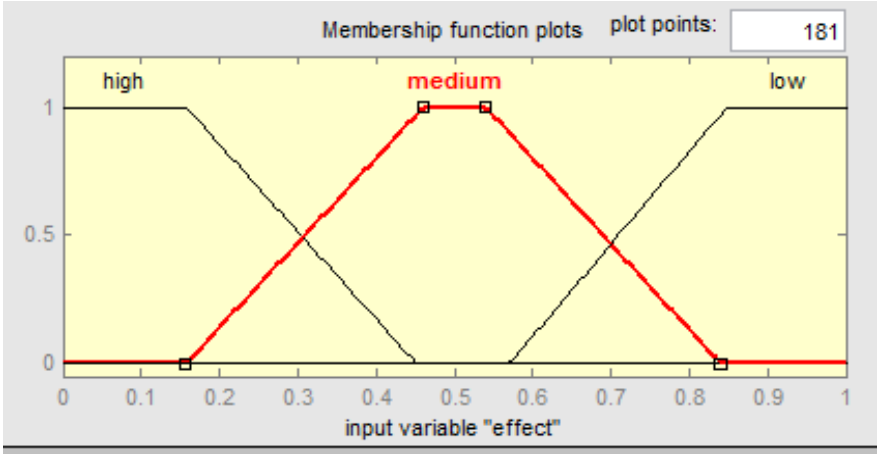

Figure 6: Effect level

In our system, the membership functions are just trapmf shaped as in Figures 2-6, the plotted functions suggest a linear transition between "true" and "false" over a certain range of values. This can be mathematically expressed as:

$$\mu_{true} = \begin{cases} 1 & , \quad x \leq 0.3 \\ 1 - \dfrac{x - 0.3}{0.3} & , \quad 0.3 < x < 0.6 \\ 0 & , x \geq 0.6 \end{cases}$$

$$\mu_{false} = \begin{cases} 0 & , \quad x \leq 0.3 \\ 1 - \dfrac{x - 0.3}{0.3} & , \quad 0.3 < x < 0.6 \\ 1 & , x \geq 0.6 \end{cases}$$

While the plotted functions suggest a linear transition "low", "medium", and high over a certain range of values, this can be mathematically expressed as:

$$\mu_{high} = \begin{cases} 0 & , \quad x \leq 0.6 \\ 1 - \dfrac{x - 0.6}{0.8 - 0.6} & , \quad 0.6 < x \leq 0.8 \\ 1 & , x > 0.8 \end{cases}$$

$$\mu_{medium} = \begin{cases} 0 & , \quad x \leq 0.2 \; or \; x \geq 0.8 \\ \dfrac{x - 0.2}{0.5 - 0.2} & , \quad 0.2 < x \leq 0.5 \\ \dfrac{0.8 - x}{0.8 - 0.5} & , x \geq 0.5 < x < 0.8 \end{cases}$$

$$\mu_{low} = \begin{cases} 1 & , \quad x \leq 0.2 \\ 1 - \dfrac{0.4 - x}{0.4 - 0.2} & , \quad 0.2 < x \leq 0.4 \\ 0 & , x > 0.4 \end{cases}$$

Figures from 2 to 6 represent membership functions in a fuzzy logic system. Each plot shows how an input variable (e.g., x, y, z, m, or effect) maps to degrees of membership in different fuzzy sets (e.g., true, false, high, medium, low).

In addition to experimenting with the application criteria. The range starts at 0 and ends at 1, as was previously mentioned is derived mathematically.

Following the input values' fuzzification stage, the produced fuzzified values are utilized to assess the rules and determine a sender's trust level (Trust level). Many fuzzy IFTHEN rules are present in the fuzzy rule base. As in the following examples:

Rule 1:

IF the timestamp is true (fresh) AND ID is true AND location is true AND behavior is true AND effect is high THEN trust level is no hack

Rule 2:

IF the timestamp is true (fresh) AND ID is true AND location is true AND behavior is false AND effect is high THEN trust level is no hack.

These rules help evaluate trust dynamically using fuzzy logic, allowing gradual transitions between trust levels instead of binary decisions.

Table 1: Fuzzy inference engine

Rule no.	timestamp	ID node	location	Vehicle behavior	Effect	Trust level
Rule1	True	True	True	True	high	No hack
Rule2	True	True	True	false	high	No hack
Rule3	True	True	false	True	high	No hack
Rule4	True	True	False	False	high	No hack
Rule5	True	False	True	True	High	No hack
Rule6	True	False	True	false	high	No hack
Rule7	True	False	false	True	high	No hack
Rule8	True	False	False	False	high	Hack
Rule9	True	True	True	True	Medium	No hack
Rule10	True	True	True	false	Medium	No hack
Rule11	True	True	false	True	Medium	No hack
Rule12	True	True	False	False	Medium	Hack
Rule13	True	False	True	True	Medium	No hack
Rule14	True	False	True	false	Medium	Hack
Rule15	True	False	false	True	Medium	Hack
Rule16	True	False	False	False	Medium	Hack
Rule17	True	True	True	True	Low	No hack
Rule18	True	True	True	false	Low	No hack
Rule19	True	True	false	True	Low	No hack
Rule20	True	True	False	False	Low	Hack
Rule21	True	False	True	True	Low	Hack
Rule22	True	False	True	false	Low	hack
Rule23	True	False	false	True	Low	Hack
Rule24	True	False	False	False	Low	hack
Rule25	False	True	True	True	high	No hack
Rule26	False	True	True	false	high	No hack
Rule27	False	True	false	True	high	No hack
Rule28	False	True	False	False	high	Hack
Rule29	False	False	True	True	High	No hack
Rule30	False	False	True	false	high	Hack
Rule31	False	False	false	True	high	hack
Rule32	False	False	False	False	high	Hack
Rule33	False	True	True	True	Medium	No hack
Rule34	False	True	True	false	Medium	No hack
Rule35	False	True	False	True	Medium	No hack
Rule36	False	True	False	False	Medium	Hack
Rule37	False	False	True	True	Medium	No hack
Rule38	False	False	True	false	Medium	Hack
Rule39	False	False	False	True	Medium	Hack
Rule40	False	False	False	False	Medium	Hack
Rule41	False	True	True	True	Low	No hack
Rule42	False	True	True	false	Low	Hack
Rule43	False	True	False	True	Low	Hack
Rule44	False	True	False	False	Low	Hack
Rule45	False	False	True	True	Low	Hack
Rule46	False	False	True	false	Low	Hack
Rule47	False	False	false	True	Low	Hack
Rule48	False	False	False	False	Low	Hack

The fuzzy inference engine used to assess the Trust level is displayed in Table 1. Every input parameter x, y, z, m is made up of two fuzzy sets (true and false) while the effect comprises three fuzzy sets (Low, Medium, and High). We create a rule table with forty-eight (48) IF-THEN rules based on the parameters to specify the trust level following the step of fuzzification. The number of fuzzy sets linked to each input parameter and the number of input parameters itself determine the number of rules. The most common rules that can be implemented are:

$$\text{No.rule}=\prod_{i=1}^{\infty}\alpha = 2*2*2*2*3 = 48$$

where α is the number of fuzzy sets of inputs, and ∞ the number of inputs.
Defuzzification, the last phase, determines the Trust level's value. We take into consideration the centroid defuzzification technique in our system model. The center of gravity and center of defuzzification region are other names for this technique. This method is the most widely applied and is fairly accurate.

$$trust = \frac{\int x_i \ \mu(x_i)}{\int \mu(x_i)}$$

Where :
xi : represents input (fuzzy value)
$\mu(x_i)$: represent the membership functions, and$\mu(x_i) = \sum_{i=1}^{n} w_i \mu_i$, where w_i represents the weight
trust: represents defuzzified value
This model is probably a component of a cybersecurity fuzzy inference system that uses TrustLevel to identify hacking attempts. Depending on the membership values, the output could be used to initiate actions (such as sending notifications or permitting or prohibiting access), as seen in Figure 7 below:

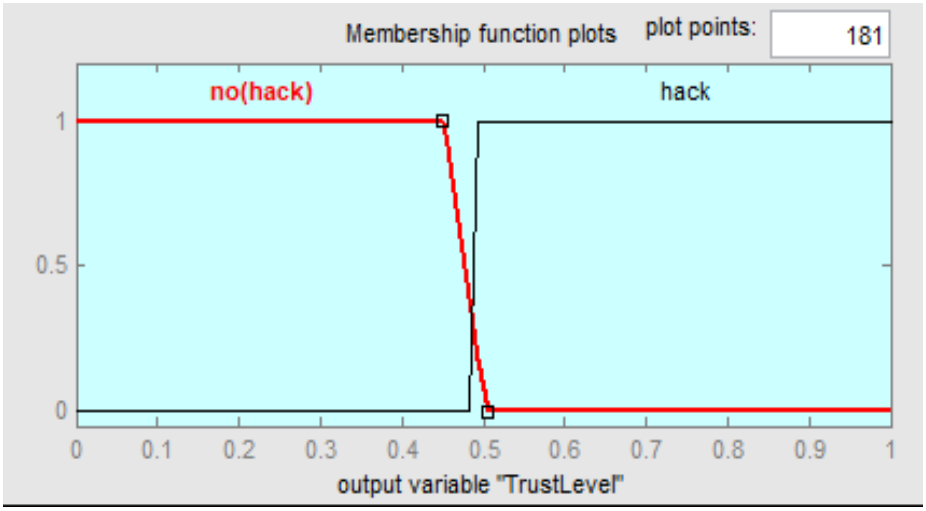

Figure 7: trust level

The proposed fuzzy logic-based authentication method offers an acceptable way to lessen the security flaws present in VANETs. The results demonstrate how the protocol may provide robust communication channels and authentication, enhancing the overall security and dependability of VANETs.

4. SIMULATION RESULTS AND DISCUSSIONS

The preliminary tests that were carried out to verify the accuracy of the proposed model are explained here.

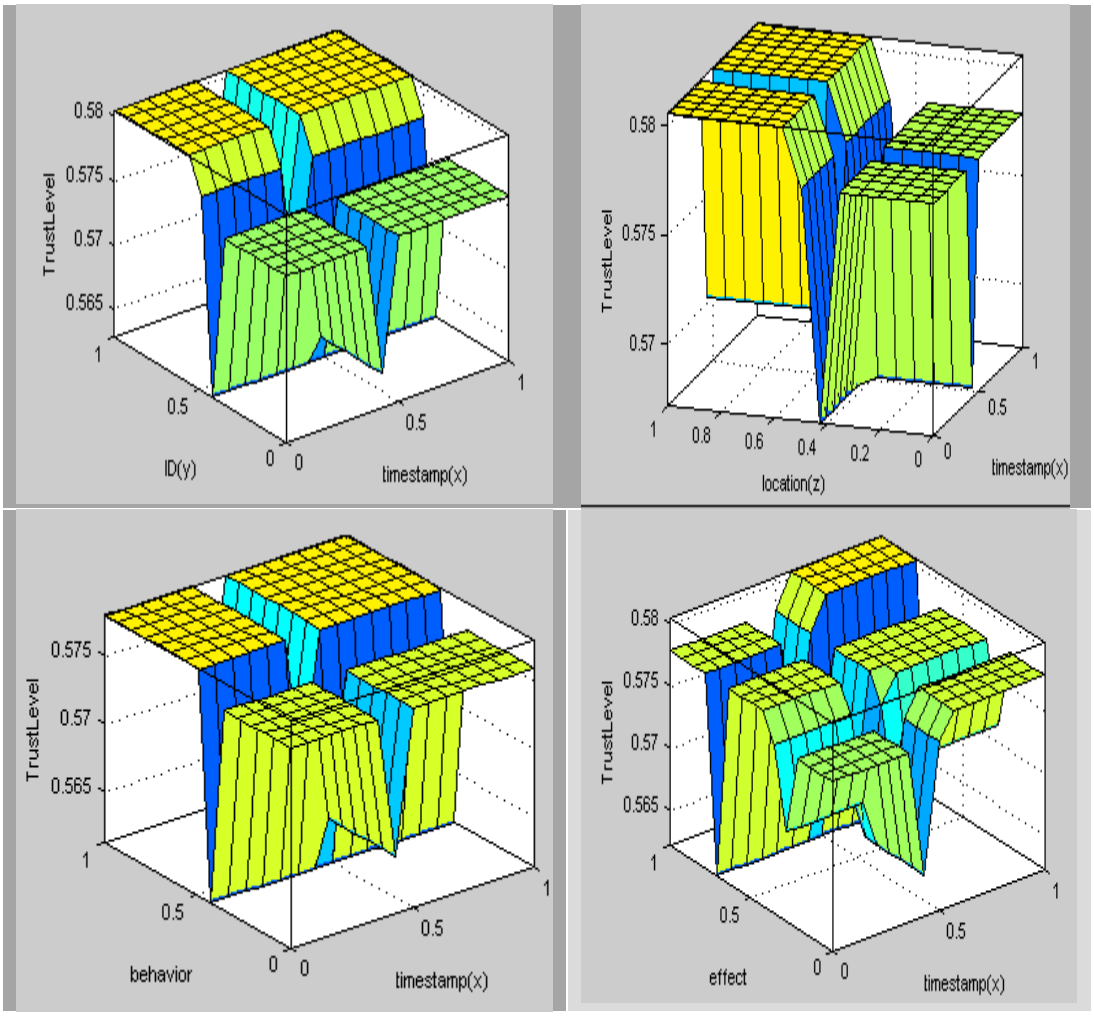

Figure 8: input-output correlation

Figure 8 displays the correlation behavior between the input and output variables. The pattern shows that the value of the output trust level increases when x is between 0.5 and 1 and other inputs are between 0.6 and 1. Therefore, inputs rise or vice versa, our fuzzy inference system may be able to enhance trust levels.

The fuzzy inference engine seen in Figure 9 below is used to calculate the "decision level" according to the rule in table 1 above:

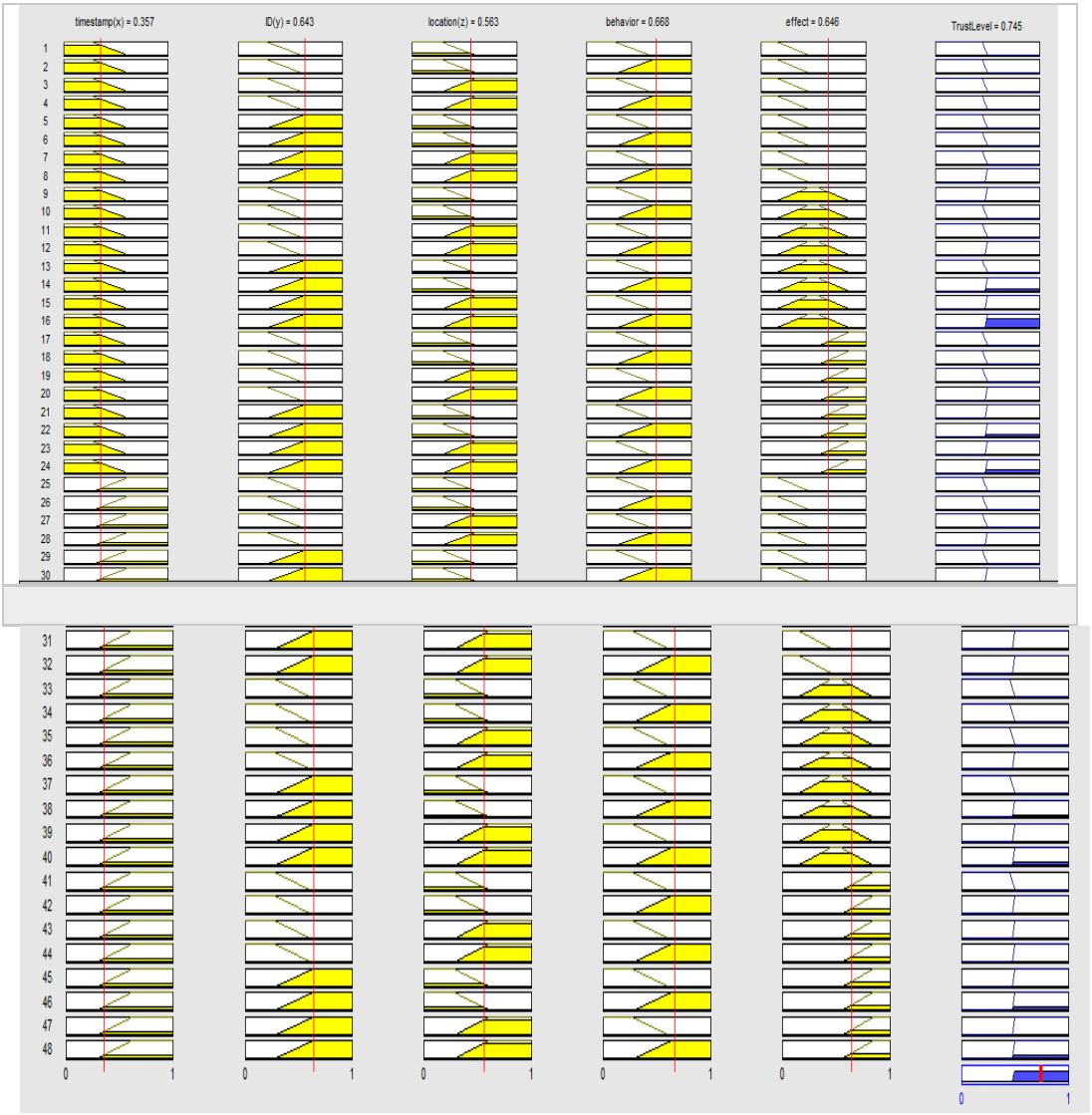

Figure 9: Fuzzy Rule Base

A number of metrics or variables from several cases or observations are visualized in the figure. Visualizing the distribution, variability, and trends of several variables over a collection of observations appears to be the primary goal of this picture. In data analysis, these kinds of visualizations are frequently employed to swiftly spot trends, correlations, or abnormalities within the dataset. Without digging into the raw data, viewers can quickly understand important insights thanks to this figure's concise synthesis of several variables. Additionally, it is simpler to examine relationships between variables when all of them are displayed side by side, such as how changes in one variable. Using this figure, the decision-makers can prioritize activities based on the insights gained, pinpoint areas of concern, and spot significant patterns. Data integrity can also be verified using the figure. For example, a variable may reveal problems like missing or corrupted data if it exhibits odd patterns (such as missing distributions).

4.1 Simulation

The validation of the proposed FBSR algorithm is done through simulation experiments in MATLAB, which includes pre-simulation environment with the Vehicle Dynamics Simulation Environment package(VDSE). The simulation parameters are listed in Table 2. For experiments, up to 80 vehicles spread over 1500 meters of road length are considered and

the number of nodes is not constant in VANET since the vehicles move at high speed. The node speed varies between 3-8 meters per second. Simulation of the proposed framework is considered only in a two-lane road. The Processor Intel Core i7, RAM: 32GB, and Storage SSD 1TB

Table 2: displays the simulation's parameters and details

PARAMETER	VALUE
ROAD LENGTH	1500
NUMBER OF NODE	80
SPEED	3-8MPs
CARRIER FREQUENCY	5.9GHz
BANDWIDTH	10MHz
MAC PROTOCOL	802.11

4.2. Performance metrics

4.2.1 Coverage percentage:

For the coverage ratio calculation, the following basic mathematical formula can be created using the method outlined:
Coverage Ratio = (Number of Covered Nodes / Total Nodes) × 100%
What:
The number of nodes whose midpoints fall inside the circular coverage cells is known as the "number of covered nodes."
The total number of nodes is the number of nodes in the target area.

4.2.2 Energy consumption:

A technique for scheduling that chooses a small number of nodes to be active at a specific moment while the rest are in a sleep state can be utilized, assuming that every node in the network is always active. Periodically, active and sleep nodes are switched to guarantee that the network is covered throughout, and that power usage is balanced.
To determine energy usage, a straightforward formula can be applied:

$$E_T = \sum_{i}^{n_\alpha} E_i \sum_{j}^{n_\beta} E_j$$

Where:
E_T : Total energy consumption
E_i: Power consumed by node i when active
E_j : Power consumed by node j when it is in idle mode
n_α : Number of active nodes
n_β : Number of sleep nodes

4.3 Performance comparison

In this section, we will show the performance of the proposed method by comparing the it with the other methods, as in Table 3

Table 3: performance comparison

Feature	**An Anonymous and Efficient Certificate** [33]	**EBCPA: for VANETs**[34]	**PKI-SC: for authentication in VANETs**[35]	**Suggest method**
Approach	verifies using digital certificates	Verifies using blockchain	uses a central CA to provide car public-private key pairs.	employs fuzzy logic to evaluate several of the parameters.
Real-Time Performance	Certificate validation may cause latency	Slower because of transaction validation and blockchain consensus	High latency because of digital signatures and other encryption/decryption processes	Lightweight fuzzy logic processes result in excellent real-time performance.
cost	High cost because of revocation and certificate management	High cost because of consensus techniques and blockchain management	High because of the centralized infrastructure, key pair generation, and oversight	Minimal computational and communication costs, requiring no extensive encryption or storage
attack	vulnerable, compromised certificates or attacks on the CA	The tamper-proof nature of blockchain makes it resistant to the majority of attacks.	Vulnerable to attacks aimed at the CA or compromised key pair	provides a flexible trust model

The performance analysis shows that our proposed scheme performs better than existing user authentication schemes.

5. Conclusions

In this paper, we proposed a trust management system for vehicular ad hoc networks (VANETs) using fuzzy logic to enhance message verification efficacy. Our simulations demonstrated that the proposed trust model effectively performs security checks to ensure the accuracy and reliability of information gathered from authorized vehicles.

Based on assessing recent developments in VANET security, we identified and defined key design requirements for trust models. Experimental results confirmed the accuracy and effectiveness of our approach in detecting malicious attacks and malfunctioning nodes. By leveraging fuzzy logic, our system efficiently manages imprecise and uncertain information in dynamic vehicular environments, ensuring precise trust evaluations.

Compared to other models, our fuzzy logic-based authentication system offers significant advantages, including real-time performance, scalability for large and dynamic networks, adaptability to the unpredictable nature of VANETs, and cost-efficiency without heavy encryption or blockchain maintenance. These attributes make our model a robust and practical solution for enhancing security and trust management in VANETs.

Acknowledgment

The Computer Science College at Qadissiya University provided the authors with invaluable help and encouragement during the study and publishing of this paper, for which they are grateful.

References

[1] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," *Telecommun. Syst.*, vol. 50, pp. 217–241, 2012.

[2] I. Seth, K. Guleria, and S. N. Panda, "A comprehensive review on vehicular ad-hoc networks routing protocols for urban and highway scenarios, research gaps and future enhancements," *Peer-to-Peer Netw. Appl.*, pp. 1–33, 2024.

[3] H. T. Cheng, H. Shan, and W. Zhuang, "Infotainment and road safety service support in vehicular networking: From a communication perspective," *Mech. Syst. Signal Process.*, vol. 25, no. 6, pp. 2020–2038, 2011.

[4] A. Raza, S. H. R. Bukhari, F. Aadil, and Z. Iqbal, "An UAV-assisted VANET architecture for intelligent transportation system in smart cities," *Int. J. Distrib. Sens. Networks*, vol. 17, no. 7, p. 15501477211031750, 2021.

[5] N. B. Jarah, "Suggesting multipath routing and dividing the zone to process communication failure in Ad Hoc networks," *Iraqi J. Sci.*, 2021.

[6] S. Baras, I. Saeed, H. A. Tabaza, and M. Elhadef, "VANETs-based intelligent transportation systems: An overview," *Adv. Comput. Sci. Ubiquitous Comput. CSA-CUTE 17*, pp. 265–273, 2018.

[7] M. Ashraf, H. Bilal, I. A. Khan, and F. Ahmad, "Vanet challenges of availability and scalability," *VFAST Trans. Softw. Eng.*, vol. 4, no. 1, pp. 46–53, 2016.

[8] M. AlMarshoud, M. Sabir Kiraz, and A. H. Al-Bayatti, "Security, privacy, and decentralized trust management in VANETs: a review of current research and future directions," *ACM Comput. Surv.*, vol. 56, no. 10, pp. 1–39, 2024.

[9] S. H. A. Kharofa, "Counting the Cells Based on Their Size Using Fuzzy Logic and the Image J System," *Iraqi J. Sci.*, pp. 2198–2210, 2024.

[10] M. S. Mahmood, "Hybrid fuzzy logic and artificial bee colony algorithm for intrusion detection and classification," *Iraqi J. Sci.*, vol. 57, no. 1A, pp. 241–252, 2016.

[11] F. Li and Q. Shen, "Introduction to Fuzzy Sets, Fuzzy Logic, and Fuzzy Inference Systems," in *Fuzzy Rule-Based Inference: Advances and Applications in Reasoning with Approximate Knowledge Interpolation*, Springer, 2024, pp. 1–15.

[12] E. QAFZEZI, "Management and Coordination of Resources in Software-Defined Vehicular Networks: Implementation and Performance Evaluation of an Integrated Fuzzy-based System and a Testbed," 2023.

[13] C. Papakostas, C. Troussas, and C. Sgouropoulou, "Fuzzy Logic for Modeling the Knowledge of Users in PARSAT AR Software," in *Special Topics in Artificial Intelligence and Augmented Reality: The Case of Spatial Intelligence Enhancement*, Springer, 2024, pp. 65–91.

[14] M. Pérez-Gaspar, J. Gomez, E. Bárcenas, and F. Garcia, "A fuzzy description logic based IoT framework: Formal verification and end user programming," *PLoS One*, vol. 19, no. 3, p. e0296655, 2024.

[15] N. Shoaip, S. El-Sappagh, T. Abuhmed, and M. Elmogy, "A dynamic fuzzy rule-based inference system using fuzzy inference with semantic reasoning," *Sci. Rep.*, vol. 14, no. 1, p. 4275, 2024.

[16] G. Finch, *Linguistic terms and concepts*. Springer, 2000.

[17] F. Li, "Fuzzy Rule-Based Inference: Advances and Applications in Reasoning with Approximate Knowledge Interpolation," 2024.

[18] J. John and K. John Singh, "Trust value evaluation of cloud service providers using fuzzy inference based analytical process," *Sci. Rep.*, vol. 14, no. 1, p. 18028, 2024.

[19] Z. Huang, Y. Yan, Y. Zhu, J. Shao, J. Zhu, and D. Fang, "Fuzzy inference system enabled neural network feedforward compensation for position leap control of DC servo motor," *Sci. Rep.*, vol. 14, no. 1, p. 20814, 2024.

[20] M. Emadi, F. Z. Boroujeni, and J. Pirgazi, "Improved Fuzzy Cognitive Maps for Gene Regulatory Networks Inference Based on Time Series Data," *IEEE/ACM Trans. Comput.*

Biol. Bioinforma., 2024.

[21] B. Zhou, Z. Liu, and H. Su, "5G Networks Enabling Cooperative Autonomous Vehicle Localization: A Survey," *IEEE Trans. Intell. Transp. Syst.*, 2024.

[22] C. Dumitrescu, P. Ciotirnae, and C. Vizitiu, "Fuzzy logic for intelligent control system using soft computing applications," *Sensors*, vol. 21, no. 8, p. 2617, 2021.

[23] S. H. Khairuddin, M. H. Hasan, M. A. Hashmani, and M. H. Azam, "Generating clustering-based interval fuzzy type-2 triangular and trapezoidal membership functions: A structured literature review," *Symmetry (Basel).*, vol. 13, no. 2, p. 239, 2021.

[24] H. Bandemer and S. Gottwald, *Fuzzy sets, fuzzy logic, fuzzy methods*. Wiley Chichester, 1995.

[25] R. Kait, S. Kaur, P. Sharma, C. Ankita, T. Kumar, and X. Cheng, "Fuzzy logic-based trusted routing protocol using vehicular cloud networks for smart cities," *Expert Syst.*, p. e13561, 2024.

[26] M. Gayathri and C. Gomathy, "FATS (Fuzzy Authentication to Provide Trust-Based Security) in VANET to Mitigate Black Hole Attack," in *Data analytics for Internet of Things infrastructure*, Springer, 2023, pp. 55–75.

[27] M. M. Hasan, M. Jahan, and S. Kabir, "A trust model for edge-driven vehicular ad hoc networks using fuzzy logic," *IEEE Trans. Intell. Transp. Syst.*, 2023.

[28] P. Patankar, S. Dorle, W. V Patil, and S. C. Patil, "A Novel AI-based Approach for the Design of VANET Communication Protocol," in *2024 International Conference on Innovations and Challenges in Emerging Technologies (ICICET)*, 2024, pp. 1–7.

[29] G. Jakobson and M. Weissman, "Real-time telecommunication network management: extending event correlation with temporal constraints," in *Integrated Network Management IV: Proceedings of the fourth international symposium on integrated network management, 1995*, 1995, pp. 290–301.

[30] C. Zhang, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 57, no. 6, pp. 3357–3368, 2008.

[31] W. Ahmad, G. Husnain, S. Ahmed, F. Aadil, and S. Lim, "Received Signal Strength-Based Localization for Vehicle Distance Estimation in Vehicular Ad Hoc Networks (VANETs)," *J. Sensors*, vol. 2023, no. 1, p. 7826992, 2023.

[32] F. B. Günay, E. Öztürk, T. Çavdar, Y. S. Hanay, and A. ur R. Khan, "Vehicular ad hoc network (VANET) localization techniques: a survey," *Arch. Comput. Methods Eng.*, vol. 28, pp. 3001–3033, 2021.

[33] Z. Qiao *et al.*, "An Anonymous and Efficient Certificate-Based Identity Authentication Protocol for VANET," *IEEE Internet Things J.*, 2023.

[34] C. Lin, X. Huang, and D. He, "EBCPA: Efficient blockchain-based conditional privacy-preserving authentication for VANETs," *IEEE Trans. Dependable Secur. Comput.*, vol. 20, no. 3, pp. 1818–1832, 2022.

[35] S. C. Sakhreliya and N. H. Pandya, "PKI-SC: Public key infrastructure using symmetric key cryptography for authentication in VANETs," in *2014 IEEE International Conference on Computational Intelligence and Computing Research*, 2014, pp. 1–6.