FATS (Fuzzy Authentication to Provide Trust-Based Security) in VANET to Mitigate Black Hole Attack

M. Gayathri and C. Gomathy

1 Introduction

VANET is derived from the concept of the MANET Mobile networking. In mobile ad hoc networks, cell phones are used in communication, and in VANET, vehicles are used for communication [1]. The concept of distributed network computing is used in VANET. Smart transportation or intelligent transportation is only possible by VANET communication technology. VANET provides a wireless mode of communication between vehicles. This type of communication allows the vehicle node to connect to another unknown vehicle node and share needed information [2]. VANET users can share information about nearby fuel stations, hospitals, ATM centers, and so on. If a road is blocked by traffic due to an accident, VANET users can intimate the other user to take a diversion to another road which will reduce the road blockage. It can even intimate about the pre-crash warning, share the emergency information, and seek help from the other node user. All these applications provide a way to a smart transportation system. VANET communicates utilizing wireless communication by broadcasting messages. When a wireless mode of communication is used, secure mechanism plays a significant role. All messages being transmitted are broadcasted messages and the hackers may secretly listen to the conversation between vehicle users and steal the information. The hackers can hack the communication and inject false messages and forward them to the destination to divert the user. The attackers can even cause a car accident by inter-operating a false message in the communication link [3]. Security mechanisms and services play a big part in vehicular communication. The onboard unit, application unit, roadside unit, and trusted authority make up the VANET architecture. Vehicles

M. Gayathri (✉) · C. Gomathy
Electronics and Communication Engineering, College of Engineering and Technology, SRM Institute of Science and Technology, Vadapalani campus, Chennai, Tamilnadu, India
e-mail: gm0717@srmist.edu.in; gomathyc@srmist.edu.in

R. Sharma et al. (eds.), *Data Analytics for Internet of Things Infrastructure*,
Internet of Things, https://doi.org/10.1007/978-3-031-33808-3_4

and roadside equipment can communicate, thanks to WAVE (Wireless Access in Vehicular Environment) [4]. Roadside units are positioned by the sides of the road to offer local connectivity to any passing vehicles. For communication, IEEE 802.11p radio technology-based DSRC-dedicated short-range communication protocols are employed [5]. Every car has onboard electronics. It comprises a GPS-based tracking gadget that transmits data to a roadside unit and other VANET node users. Vehicles are furnished with an event data recorder, an onboard unit, and sensors that give information to the other vehicle nodes [6, 7]. Communication via the VANET network is secured in large part by trusted authority. All of the vehicle's onboard identities are registered by a reliable authority, which then transmits that data to the roadside device. Before opening a communication channel with other nodes, it authenticates the vehicle, the user, and the user's identity. Together, these pieces of technology offer a communication link between vehicles as well as between vehicles and roadside equipment, infrastructure, pedestrians, and even train users. On the basis of trust models, many trust-based authentication systems are addressed in [8]. Trusted approach provides a highly secure communication. Section 2 discusses in brief about VANET architecture, Sect. 3 discusses the various attacks and threats generated in VANET, Sect. 4 explains the views on the prominent issues caused by black hole node, Sect. 5 concentrates on the fuzzy logic and its role in the proposed approach, Sect. 6 explains the proposed algorithm FATS, and Sect. 7 gives a brief note on implementation of algorithm in ns 2.28 software. Parameter estimation, framing of rules in MATLAB for detecting black hole attacks, and networking are done using ns 2.28 software [9].

2 VANET Architecture

Vehicular ad hoc networking is being introduced to provide intelligent transportation and minimize road accidents. Vehicle node consists of numerous sensors and actuator that enable the vehicle to sense the vehicle, pedestrian in its 360-degree range, and act based upon the road conditions. The major components used in VANET communication are vehicle node, onboard unit, road side unit, Trusted Authority required to communicate between vehicles, pedestrian, and other infrastructures. Onboard units are built inside the smart cars which are used in the communication these devices serve as a transceiver between the source and the destination [10]. The Certificate Authority is crucial in ensuring verified and secure communication between vehicles. In internet connected with all components of the VANET, it is very important to pay attention on providing security and privacy in the VANET networking. Hackers or attackers would try to steal the information and collapse or the smooth functioning of the network by inducing false message in the stream that would result in the crashing between vehicles, create traffic, can divert the user by modifying his/her location, and so on. Certificate authorities are third-party authority responsible for producing genuine certificate to the user based on the identity and behavior of the node. Figure 1 describes the architecture of the

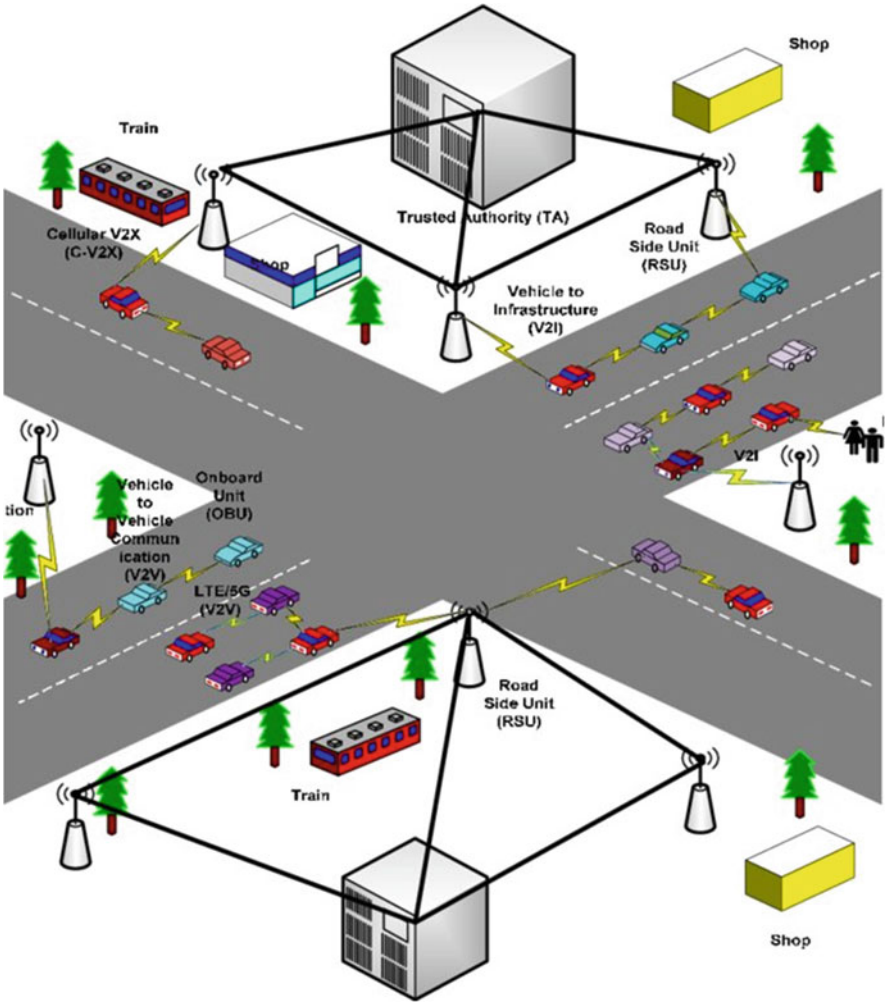


Fig. 1 VANET architecture

VANET. As was already mentioned, its main components are smart automobiles, roadside units, and trusted authorities. It is feasible for vehicles to communicate with each other, with pedestrians, with roadside equipment, with infrastructure, and even with other vehicles [11].

Vehicle-to-vehicle communication is possible because of the DSRC protocol (Dedicated Short Range Communication).

3 Attacks and Threats Generated in VANET

The attacks being generated in VANET can be classified based on availability, confidentiality, authentication, integrity, and non-repudiation [4, 12]. These attacks in VANET occur in different security layers. The attacks generated while routing is done in the vehicle node are called routing attacks. Routing attacks are classified into selfish node attacks, jellyfish attacks, data flooding attacks, data alteration attacks, and black hole attacks [13].

3.1 Selfish Node Attack

In this attack, the node will behave as a self-obsessed node. If it is been contacted to share the information with the other node, it will either send or drop the packets to save its resource. It will not share the information genuinely. The selfish node will try to save the available resource for its use [14]. This will result in a wastage of resources and bandwidth [15].

3.2 Jellyfish Attack

Jellyfish attack normally introduces a delay in the attack by introducing itself as a genuine node. It tries to deny the service and delay the message being transmitted to the destination around 0–10 s. This attack affects both the TCP layer and the UDP layer. Since a jellyfish attack delays the message, it creates wastage of resources, increases bandwidth, and replicates the message to create more traffic in the network [13].

3.3 Data Flooding Attack

Data flooding attack creates high congestion in network traffic. This malicious hacker selects an IP address that is not available in the network communication and tries to send unwanted messages to all the nodes using that IP address which creates high congestion and network traffic that delays the important or emergency messages that are being transmitted [16].

3.4 Black Hole Attack

A black hole attack in a VANET addresses itself as having the shortest path from the source to the destination when a route request is sent to the nodes that are available in a specific zone. The source node sends packets through the malicious node after realizing the message was a hoax. After receiving the message, the attacker will discard the packet without sending it to its intended location. A packet drop attack is another name for this black hole assault [17].

4 Prominent Issues Caused by a Black Hole Node

In VANET, numerous assaults are produced. These attacks can be divided into categories depending on assaults on confidentiality, integrity, availability, authentication, and non-repudiation. The black hole or malicious node is to blame for all of these attacks.

Black hole nodes are the main target of attack in a VANET scenario because they generate greater message transmission delays, jam communication by losing packets, or even alter data. Black hole nodes can disrupt VANET connectivity and have a negative impact on it. The proposed approach FATS- Fuzzy authentication to provide trust-based security is used to mitigate black hole attack and this approach with slight modification could be used to mitigate other attack too.

The black hole attack on VANET is depicted in Fig. 2. In order to communicate with Node D, Node A sends a Route request message to every node in the vicinity. The malevolent node, Node M, is regarded as a black hole node in this context. The time stamp and the number of hops required to get to the destination are included in the route reply message that each node sends. The malicious node M, a black node that cannot communicate with the destination node D, identifies itself by claiming

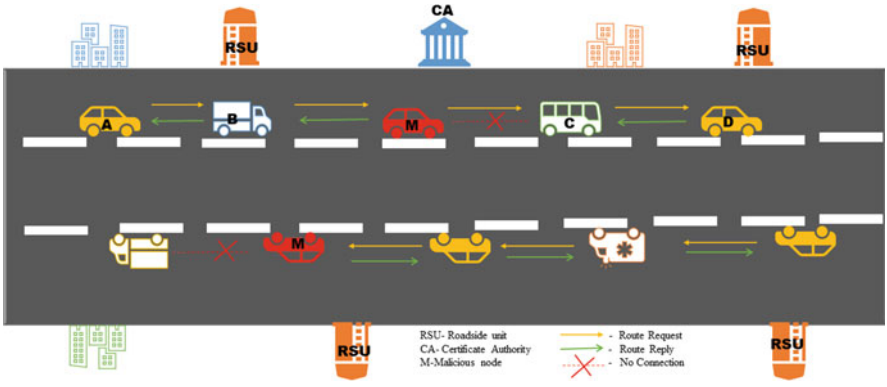


Fig. 2 Black hole attack in VANET

to have the shortest path there with the fewest hops and the earliest time stamp [18]. Node A accepts that node and transfers the data to black hole Node M. Node M drops the data packet [19]. Black hole attack can be detected based on the packet loss analysis, Traffic analysis and based on inspecting the packets being altered. This drop in the data packet increases the traffic delay of the data transfer, causes packet loss, and attacker may even inject or modify the message. If the weight of the trust factor is analyzed properly at each and every part of the node, then malicious node can be avoided from entering into the communication zone. FATS algorithm analyses the trust factor and traffic delay while transmitting the messages and detects black hole attack in VANET [20].

Ad hoc on-demand distance vector (AODV) routing protocol is used in the suggested technique. As a reactive system, AODV routing protocol offers route discovery based on demand. The AODV routing protocol locates the route and allots a path to the required source when a route request is received. The three steps of the AODV routing protocol are route discovery, data transfer, and route management. RREQ and RREP routing techniques are used by the AODV routing protocol to offer the optimum path. The source IP address, source sequence number, destination IP address, destination sequence number, and broadcast ID are all sent in RREQ query packets. The destination IP address, destination sequence number, source IP address, hop count, and lifetime of a node are included in RREP responses [21].

5 Fuzzy Logic and Its Role in the Proposed Approach

5.1 Introduction About Fuzzy Logic

A strategy that depends on the degree of truthfulness is fuzzy logic. Boolean functions can only classify anything as true or false, whereas fuzzy logic can approximate the inputs. Fuzzy logic was proposed by Lofti Zadeh [22] and is based on the concept of human approximation [23]. When a human is allowed to take a decision, apart from Yes or No, the human can take decisions such as may be, certainly yes or no, not possible, and am not sure. Boolean function is able to work only on the concept of true or false and yes or no, but fuzzy approximation will concentrate on all the possible aspects of a human being. It will act intelligently as a human being. Fuzzy logic is the base of artificial intelligence and can be implemented in both hardware and software problem [24].

Figure 3 shows the block diagram of the fuzzy logic system. The basic fuzzy logic controller has the Fuzzifier, knowledge base, inference engine, and a fuzzifier. The crisp input is fed into the fuzzifier. The fuzzifier is used to fuzzify the input based on the system model. After fuzzification of the inputs, “if then” rules are applied to the data. Knowledge base is used to apply “if then” rule to build the model of the system. Inference engine is used to get inference from the human reasoning

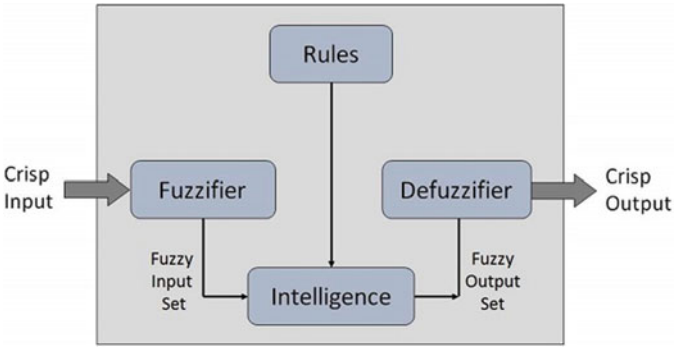


Fig. 3 Block diagram of fuzzy logic

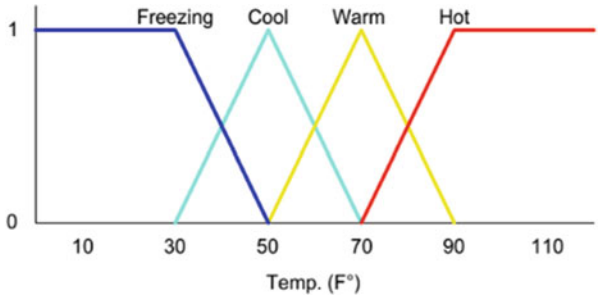


Fig. 4 Membership function of a temperature

approximation. After approximation of the model, the input is fed to the fuzzifier that are used to defuzzify the input to crisp output.

Membership function plays a significant role in quantifying the linguistic variable and in showing the fuzzy relation graphically. Figure 4 represents the membership function of the temperature. Temperature data are divided into freezing, cool, warm, and hot. In cases when there is a lot of ambiguity, fuzzy logic is applied [25].

Fuzzy logic can be divided into three types of fuzzy inference system:

- Mamdani fuzzy inference system.
- Takagi Sugeno fuzzy inference system.
- Tsukamoto fuzzy inference system.

5.2 *Mamdani Fuzzy Inference System*

Mamdani fuzzy inference system was first proposed by Ibrahim Mamdani to control steam engine. The Mamdani inference engine can be divided into two inference system [26]:

- Max-Min inference method.
- Max-product inference method.

5.2.1 Max-Min Inference Method

Consider the following rules:

Rule 1: IF x_1 is $A_1{}^1$ *and* x_2 is $A_2{}^1$ THEN y^1 is B^1.
Rule 2: IF x_1 is $A_1{}^2$ *and* x_2 is $A_2{}^2$ THEN y^2 is B^2.

Let us compute the output for $x_1 = 2.5$ and $x_2 = 3$.

Membership functions for given rules are shown below:

The highest membership value from the two input sets is assigned to the appropriate output set because it is a Max-Min inference method.

For first rule, the fuzzy membership value for x_1 would be 0.8 and for x_2 it would be 0.4. The connectives in first IF-THEN rule are connected using "and" connective. Therefore, we must find the intersection of the fuzzy values that returns the lowest value. As a result, the output y^1 will belong to fuzzy output set B1 by 0.4.

The fuzzy membership value for the second rule would be 0.3 for x_1 and 0.7 for x_2. The "or" connective is used to connect the connectives in the first IF-THEN rule. Therefore, we must use the union of fuzzy values that returns the most of them. In the fuzzy output set B2, the output y^2 will therefore have membership of 0.7. The input and output fuzzy sets and scaling of output fuzzy function are depicted in Figs. 5, 6, 7, and 8 for max-min inference method and aggregated output is shown in Fig. 9.

Fig. 5 Input fuzzy set $A_1{}^1$

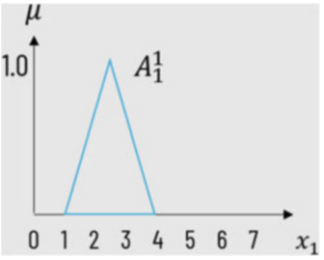


Fig. 6 Input fuzzy set $A_2{}^1$

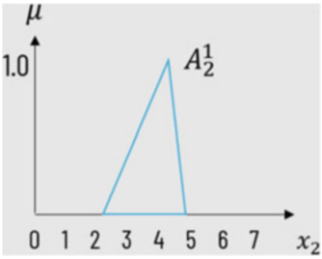
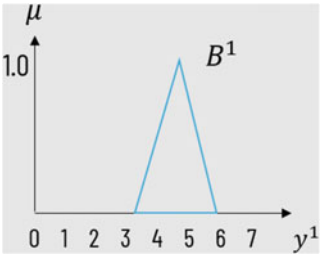


Fig. 7 Output fuzzy set B^1



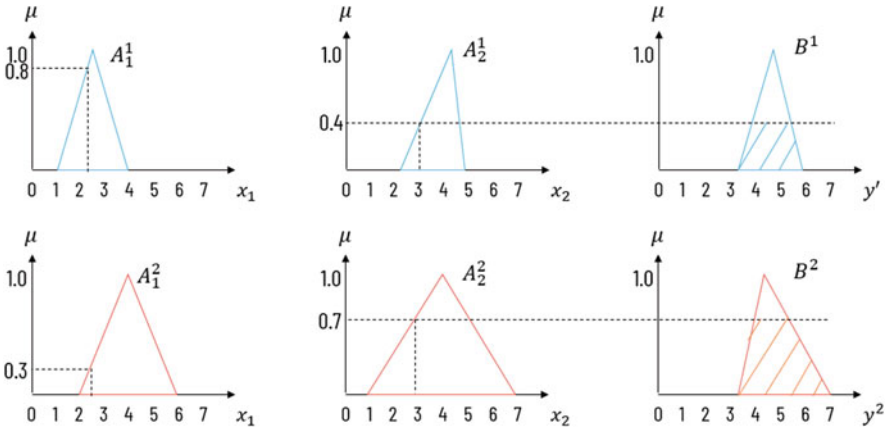
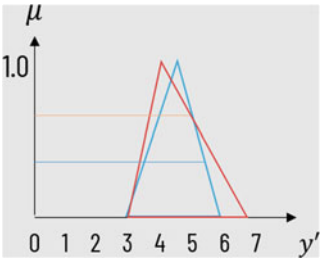


Fig. 8 Scaling of output fuzzy function

Fig. 9 Aggregated fuzzy output



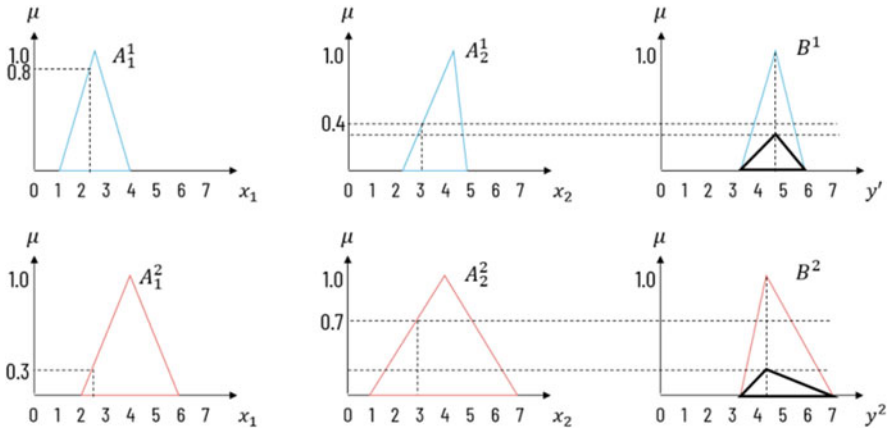


Fig. 10 Scaling of output fuzzy function

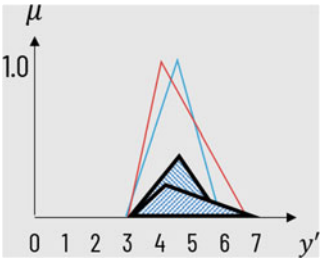


Fig. 11 Aggregated fuzzy output

5.2.2 Max-product inference method

An approach for combining fuzzy sets in fuzzy logic is the maximum product inference method. It is based on the principle that the sum of the degrees to which the components of a fuzzy set are true determines the degree to which the whole is true.

The above figure shows the representation of max-prod inference method. Figure 10 and Fig. 11 shows the scaling of output function with respect to the given input and Fig. 11 shows the aggregated fuzzy output.

6 Fuzzy Logic Trust-Based Authentication Schemes in VANET

A fuzzy-based approach for evaluating trustworthiness and managing authority in VANETs is suggested. In this chapter, the fuzzy theory was employed. To analyze the nodes' trust, it employed the behavioral attribute acquisition, vehicle device position, and comprehensive attribute weight as a parameter [27]. In the world of

uncertainty, fuzzy logic is crucial. Because of VANET's high degree of mobility, it is challenging to forecast which nodes will enter and leave the network. Fuzzy logic is used to assign a trust parameter to track the node's sincerity, making it simple to foresee the node's sincerity. A trust factor based on authentication of vehicle and roadside unit was provided by Fatemehsadat et al. Direct trust, indirect trust, in-segment trust, and historical trust were taken into consideration to calculate the trust factor of the vehicle node [28]. A trust model using experience and plausibility was proposed in fuzzy logic [8].

7 Proposed Algorithm FATS (Fuzzy Authentication to Provide Trust-Based Security) for Black Hole Attack Detection

The trust factor plays a significant role in avoiding the malicious node joining the communication link. The trust factors provided by certificate authority by monitoring vehicle identity, trust factor provided by the roadside unit, trust factor calculated by the reputation of each node which is credited based on nodes behavior, the data trust and number of hops required to reach the destination is taken as input to calculate the trust degree of providing the communication link to the requestee node. The proposed algorithm FATS (Fuzzy Authentication to provide Trust-based Security) helps to detect black hole node and block the node to do any communication further. The trust degree or the weight of the node identity, weight of the trust degree provided by RSU, weight of the direct and indirect trust degree, and weight of the data trust are calculated.

Step 1: If a new node wants to join the communicating network in VANET, the node sends the RREQ message to all the nodes. After receiving the RREQ message, the trust factors are first analyzed before joining the node to the network.

Step 2: The trust factors are separately analyzed by VANET's Certificate authority. At the initial stage, vehicles' IDs are verified – whether it is a registered node or not.

Step 3: If it is not a registered node, the genuine node can block that node from joining and leaving a message as a suspicious node.

Step 4: If the node is registered, the trust factor provided by the RSU and the trust factor provided by the reputation of each node are verified.

Step 5: If the node is found to be a genuine node, after verifying the trust degree, then the communication link is provided to the new node by replying with an RREP message.

Step 6: If the malicious node still acts as a genuine node initially, a test message is forwarded to the destination node to analyze the trusted behavior of VANET. If there is a packet drop or delay in receiving the acknowledgment message, then the node can be blocked. If the acknowledgment is received, then the original

messages which are in need to be transmitted are encrypted to ciphertext and forwarded to the destination node.

Step 7: When the new node is ready for a data transfer, trustworthiness of data is ensured by observing the previous data sent by the new node. This form of trust comes under historical trust.

7.1 Pseudocode for Providing a Communication Link to the New Node

Every vehicle i sends the RREQ route request message to join the communication link.

```
{
Verifiers verify the vehicle id
   If {
Node id is registered
}
Considered as a genuine node
 Else {
 Block the node from the communication link
}
}
If {
#genuine node is found by verifying vehicle's id
#Verify the node's reputation trust and RSU Trust
If the trust degree is reached above the threshold level
Accept the node
Else {
Reject node
}}
# Check the genuineness of the user by sending a test message If {
The test message is sent at the correct time and acknowledgment
is received
Provide a communication link by RREP message
Else {
 Report malicious
}
}
```

7.2 Formation of Fuzzy Rules Using Mamdani Inference System in MATLAB

Node reputation trust, roadside unit trust, data trust factor, and the number of hops required to reach the destination from the source are chosen as input parameters. All

Table 1 Calculation of trust values to provide a communication link

S. no	Node reputation trust	Roadside unit trust	Data trust	Number of hops required to reach the destination	Provide communication link
1	0	0	0	0	0
2	0	0.6	0.6	0.6	0.6
3	0	1	1	0	0.6
4	0.6	0	0	0	0
5	0.6	0.6	0.6	0.6	0.6
6	0.6	1	1	1	0.6
7	0.6	1	1	0	1
8	1	0	0	0	0
9	1	0.6	0.6	0.6	0.6
10	1	1	1	0.6	1
11	1	0.6	1	0.6	1
12	1	1	0.6	0	1

these parameters determine black hole attack in VANET and reject the malicious node if the trust factors are very low.

Mamdani FIS is used with IF-THEN rules. These rules are framed to select the genuine node and reject the black hole node in VANET. The centroid defuzzification method is used to calculate the trust parameter of the vehicle node. Table 1 discusses the various criteria for providing a communication link to the new node and rejecting the black hole node. Equation (1) gives the centroid defuzzification formula for calculating the trust factor. Figure 12 shows the surface view of the calculation of trust degree required to provide a communication link to the trusted node.

$$\text{Trustfactor} = \frac{\int \text{xi}.\mu\ (\text{xi})}{\int \mu\ (\text{xi})} \tag{1}$$

Figures 12 and 13 shows the trust metric calculation for the medium and low trust factor respectively. If there is a low trust factor, then communication link will be discarded to that node, and if there is a medium trust factor, then communication may be provided to that node. Figure 14 depicts the surface view for providing communication link.

8 Implementation of FATS

The network simulation software 2.28 is significantly used for the research work in VANET [29]. It is an open-source software in which simulation of wireless

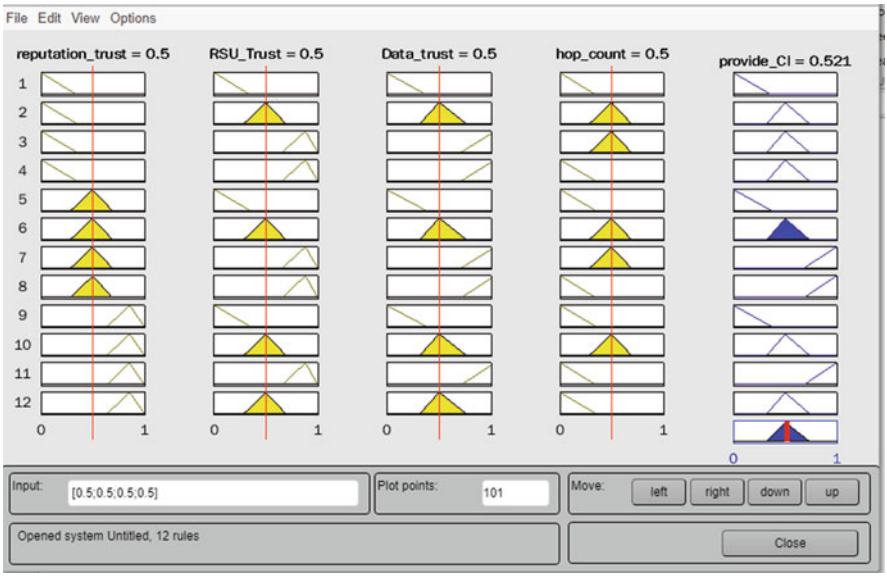


Fig. 12 Trust factor calculation for medium trust factor

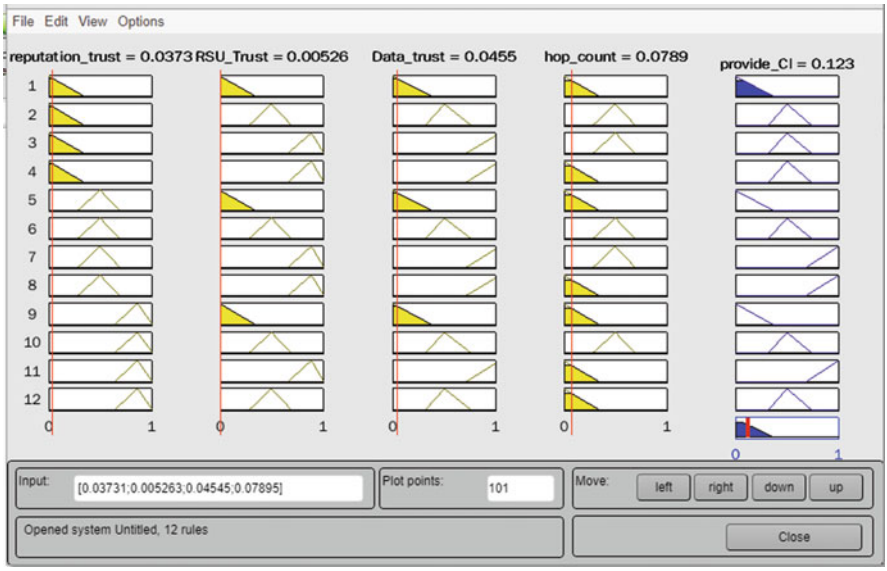


Fig. 13 Trust factor calculation for low trust factor

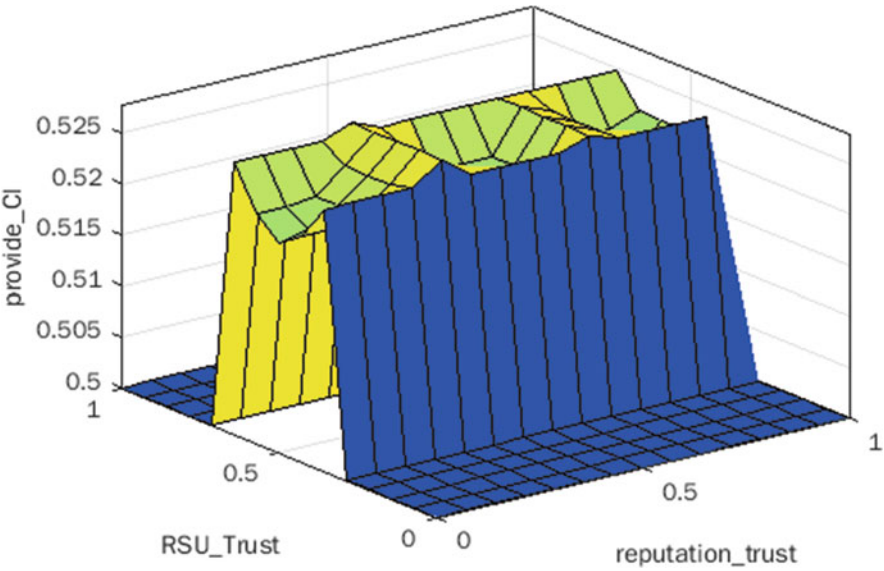


Fig. 14 Surface view for calculation of trust value to provide a communication link

applications can be done more easily. Around 100 nodes have been designed with the roadside unit and vehicle nodes.

The vehicle node moves around, and if any information is required, the user can get the information from the other node user. In this scenario, the trust factor plays a significant role; this trust factor gives the degree of whether the node which is contacted is a trusted node or not. According to Table 1, values between 0 and 0.65 are low trust values, values from 0.5 to 0.85 medium trust values, and values from 0.8 to 1 high trust values.

If the trust degree calculated is below the threshold value, the user can block that node from communication and send the request to the other node user. When the communication is initiated, messages which are transmitted are encrypted to cipher text form by using public and private key for the authentication process and key is generated to pass the information. The trust degree based on vehicle ID, the reputation of the node, and RSU trust detects black hole attack in VANET and helps the node user to discard the black node which increases the throughput and packet delivery ratio and decreases the delay ratio. Figure 3 shows the image of the ns2.28 simulation tool, which consists of vehicle nodes, roadside unit, and black hole attacks along the direction of movement of the vehicle. The fuzzy-based trusted communication detects the black hole attack and rejects the attacked node and chooses the genuine node for communication based on fuzzified trust degree. This proposed method increases the throughput and packet delivery ratio and decreases the delay time. Figure 15 shows the detection of attack in animator window of ns2.28 (Table 2).

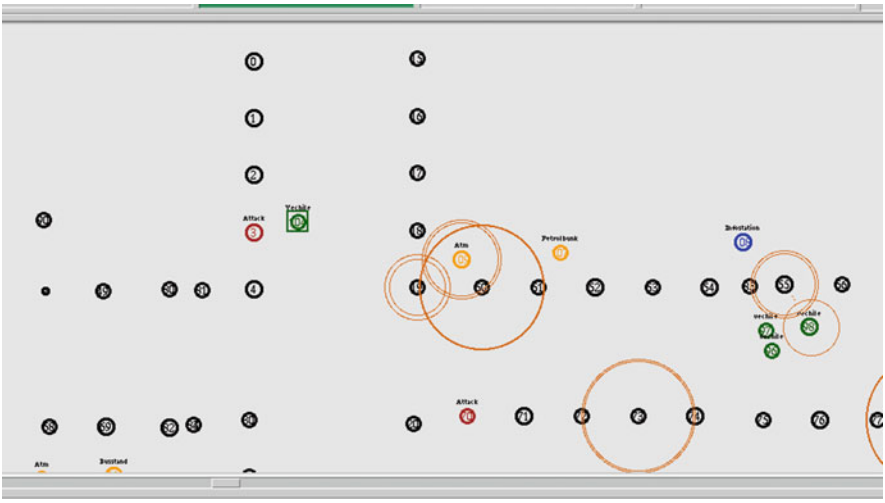


Fig. 15 Detection of black hole attack in VANET

Table 2 Depicts the simulation parameter used in this approach

Simulation tool	NS 2.28
Simulation area	1200 m × 1200 m
Routing protocol	AODV
Channel type	Wireless
Radio propagation model	Two ray ground
Packet size	64 bytes
Performance evaluation	Packet delivery ratio, throughput, and end-to-end delay

Throughput (Kbps)
Throughput is defined as the total number of packets reached at the destination to the amount of time taken.

$$\text{Throughput} = \frac{\text{Total number of packets received at the destination in bytes} \times 8}{\text{End time} - \text{Start time}}$$

Packet delivery ratio (in %) [30]
Packet delivery ratio is defined as the ratio of the total packets received at the destination to the total packets generated by the node.

$$\text{Packet delivery ratio} = \frac{\text{Packet received}}{\text{Packet generated}} \times 100$$

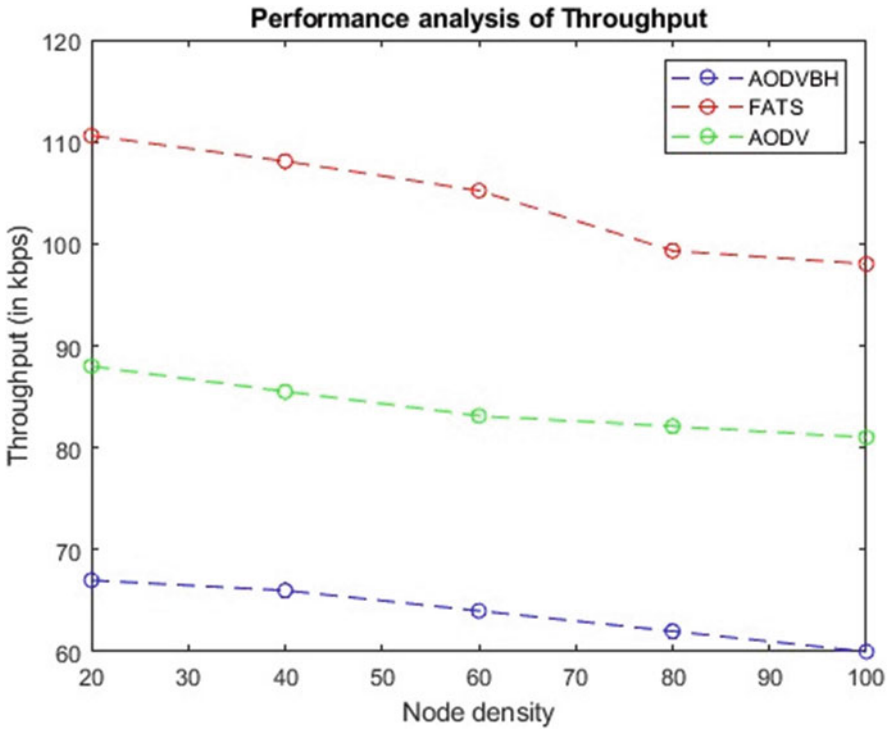


Fig. 16 Analysis of throughput performance

End-to-end delay (s)
End-to-end delay is defined as the difference between the packet sent time and packet arrival time across a network.

$$\text{End} - \text{to} - \text{end delay} = \text{Packet sent time} - \text{Packet arrival time across a network.}$$

Figures 16, 17, and 18 show the performance analysis of throughput, packet delivery ratio, and end-to-end delay performance, respectively. The performance analysis shows that Fuzzy-trusted approach increases the throughput and packet delivery ratio and decreases the delay when compared to normal AODV routing protocol and AODVBH-AODV black hole.

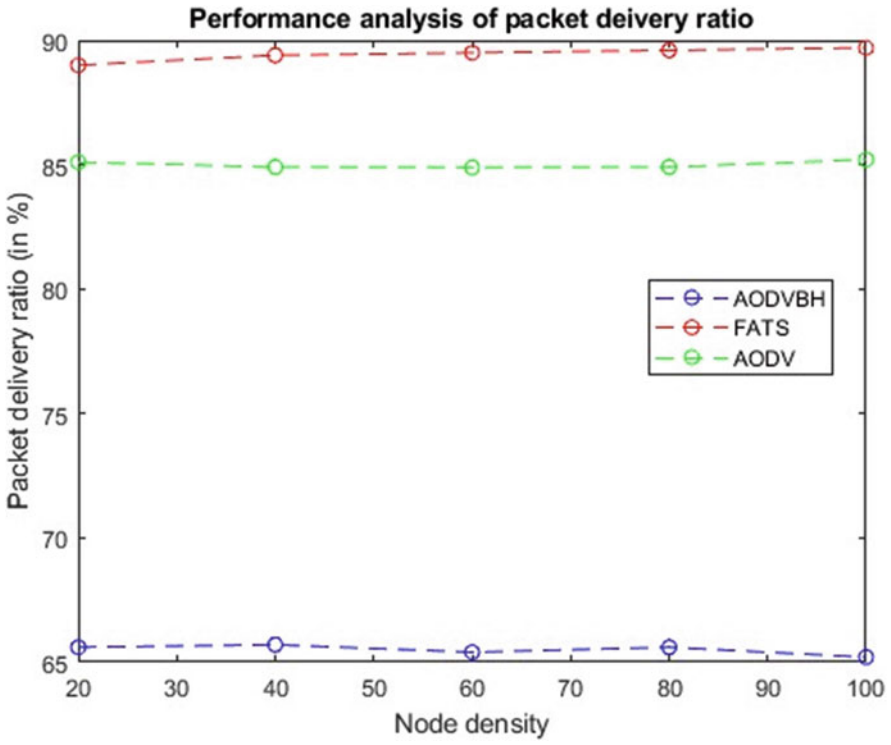


Fig. 17 Analysis of packet delivery ratio

9 Conclusion

The proposed method used FATS (Fuzzy Authentication to provide Trust-based Security) for the detection of black hole attacks in VANET. When the black hole attack is detected in VANET, the trusted authority blocks the node to join from the communication link. The trust degree plays a significant role in authenticating the user. The trust degree is calculated based on vehicle identity, roadside unit trust, node reputation trust, and data trust. This degree of trust makes the VANET user decide whether to trust the node or block the black hole node. Fuzzy logic is normally used in the scenario where there is more uncertainty. This fuzzy-based trusted authentication scheme, FATS, increases the packet delivery ratio and throughput and decreases the delay time. This proposed method increases the network lifetime and bandwidth and reduces the packet drops caused by the black hole node. Secure infrastructure is provided by this method to transfer the data packets in a secure communication network.

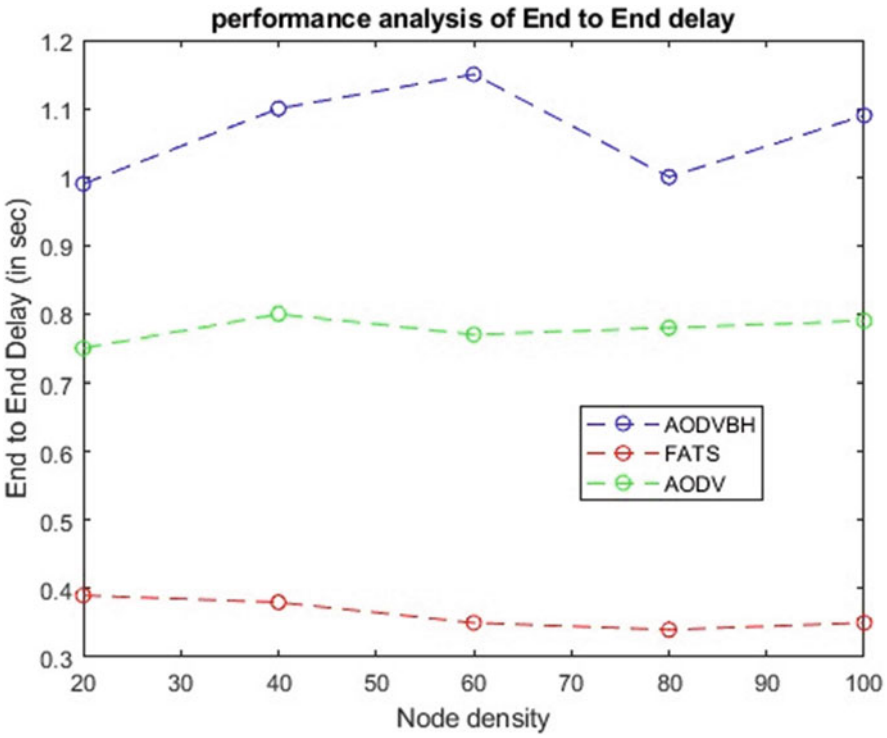


Fig. 18 Analysis of end-to-end delay performance

References

1. Cooper, C., Franklin, D., Ros, M., Safaei, F., & Abolhasan, M. (2017). A comparative survey of VANET clustering techniques. *IEEE Communications Surveys & Tutorials, 19*(1), 657–681. https://doi.org/10.1109/COMST.2016.2611524
2. Rasheed, A., Gillani, S., Ajmal, S., & Qayyum, A. (2017). Vehicular Ad Hoc Network (VANET): A survey, challenges, and applications. In *Vehicular ad-hoc networks for smart cities* (pp. 39–51). https://doi.org/10.1007/978-981-10-3503-6_4
3. Onishi, H. (2018). A survey: Engineering challenges to implement VANET security. In *2018 IEEE international conference on vehicular electronics and safety (ICVES)* (pp. 1–6). https://doi.org/10.1109/ICVES.2018.8519503
4. Sheikh, M. S., & Liang, J. (2019). A comprehensive survey on VANET security services in traffic management system. In *Wireless communications and mobile computing, 2019*.
5. Al-Sultan, S., Al-Doori, M. M., Al-Bayatti, A. H., & Zedan, H. (2014). A comprehensive survey on vehicular Ad Hoc network. *Journal of Network and Computer Applications, 37*, 380–392.
6. Azees, M., Jegatha Deborah, L., & Vijayakumar, P. (2016). Comprehensive survey on security services in vehicular adhoc networks. *IET Intelligent Transport Systems, 10*(6), 379–388.
7. Vo, M. T., Vo, A. H., Nguyen, T., Sharma, R., & Le, T. (2021). Dealing with the class imbalance problem in the detection of fake job descriptions. *Computers, Materials & Continua, 68*(1), 521–535.

8. Soleymani, S. A., et al. (2017). A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing. *IEEE Access, 5*, 15619–15629. https://doi.org/10.1109/ACCESS.2017.2733225
9. Sachan, S., Sharma, R., & Sehgal, A. (2021). Energy efficient scheme for better connectivity in sustainable mobile wireless sensor networks. *Sustainable Computing: Informatics and Systems, 30*, 100504.
10. Ghanem, S., Kanungo, P., Panda, G., et al. (2021). Lane detection under artificial colored light in tunnels and on highways: An IoT-based framework for smart city infrastructure. *Complex & Intelligent Systems*. https://doi.org/10.1007/s40747-021-00381-2
11. Sachan, S., Sharma, R., & Sehgal, A. (2021). SINR based energy optimization schemes for 5G vehicular sensor networks. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-021-08561-6
12. Gayathri, M., & Gomathy, C. (2021). A deep survey on types of cyber attacks in VANET. *JCR, 8*(1), 1029–1039. https://doi.org/10.31838/jcr.08.01.11
13. Kumar, A., Varadarajan, V., Kumar, A., Dadheech, P., Choudhary, S. S., Ambeth Kumar, V. D., Panigrahi, B. K., & Veluvolu, K. C. (2021). Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm. *Microprocessors and Microsystems, 80*, 103352., ISSN01419331. https://doi.org/10.1016/j.micpro.2020.103352
14. Ding, Q., Zeng, X., Zhang, X., & Sung, D. K. (2019). A public goods game theory-based approach to cooperation in VANETs under a high vehicle density condition. *IEEE Transactions on Intelligent Transportation Systems, 20*(11), 3995–4005.
15. Priyadarshini, I., Mohanty, P., Kumar, R., et al. (2021). A study on the sentiments and psychology of twitter users during COVID-19 lockdown period. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-021-11004-w
16. Liu, H., Chen, Y., Tian, H., Wang, T., & Cai, Y. (2016, October). A novel secure message delivery and authentication method for vehicular ad hoc networks. In *2016 first IEEE international conference on computer communication and the Internet (ICCCI)* (pp. 135–139). IEEE.
17. Azad, C., Bhushan, B., Sharma, R., et al. (2021). Prediction model using SMOTE, genetic algorithm and decision tree (PMSGD) for classification of diabetes mellitus. *Multimedia Systems*. https://doi.org/10.1007/s00530-021-00817-2
18. Priyadarshini, I., Kumar, R., Tuan, L. M., et al. (2021). A new enhanced cyber security framework for medical cyber physical systems. *SICS Software-Intensive Cyber-Physical Systems*. https://doi.org/10.1007/s00450-021-00427-3
19. Miao, T., Shen, J., Lai, C.-F., Ji, S., & Wang, H. (2021). Fuzzy-based trustworthiness evaluation scheme for privilege management in vehicular ad hoc networks. *IEEE Transactions on Fuzzy Systems, 29*(1), 137–147. https://doi.org/10.1109/TFUZZ.2020.3030490
20. Priyadarshini, I., Kumar, R., Sharma, R., Singh, P. K., & Satapathy, S. C. (2021). Identifying cyber insecurities in trustworthy space and energy sector for smart grids. *Computers & Electrical Engineering, 93*, 107204.
21. Upadhyaya, A. N., & Shah, J. S. (2019). Effect on AODV routing protocol under blackhole attack in VANET. *International Journal of Computer Engineering and Technology, 10*(3), 166–174.
22. Zadeh, L. (1978). Fuzzy sets as a basis of possibility. *Fuzzy Sets and Systems, 1*, 3–28.
23. Singh, R., Sharma, R., Akram, S. V., Gehlot, A., Buddhi, D., Malik, P. K., & Arya, R. (2021). Highway 4.0: Digitalization of highways for vulnerable road safety development with intelligent IoT sensors and machine learning. *Safety Science, 143*, 105407. ISSN 0925-7535.
24. Luo, Q., Cai, X., Luan, T., et al. (2018). Fuzzy logic-based integrity-oriented file transfer for highway vehicular communications. *EURASIP Journal on Wireless Communications and Networking, 2018*, 3. https://doi.org/10.1186/s13638-017-1009-x
25. Sahu, L., Sharma, R., Sahu, I., Das, M., Sahu, B., & Kumar, R. (2021). Efficient detection of Parkinson's disease using deep learning techniques over medical data. *Expert Systems*, e12787. https://doi.org/10.1111/exsy.12787

26. Codecrucks. (2021, August 22). Mamdani fuzzy inference System-Concept-CodeCrucks. *CodeCrucks*. https://codecrucks.com/mamdani-fuzzy-inference-concept/
27. Gautham, P. S., & Shanmughasundaram, R. (2017). Detection and isolation of black hole in VANET. In *2017 international conference on intelligent computing, instrumentation and control technologies (ICICICT)* (pp. 34–1539). https://doi.org/10.1109/ICICICT1.2017.8342799
28. Mirsadeghi, F., Kuchaki, M., & Gupta, R. B. B. (2020). *A trust infrastructure-based authentication method for clustered vehicular ad hoc networks*. Springer Science+Business Media, LLC, part of Springer Nature.
29. Li, J., Zhang, Y., Zhao, J., Wang, Y., Ma, X., & Wu, W. (2017). NS-2 simulation of VANET for safety applications. In *Proceedings of the 8th international conference on computer modeling and simulation - ICCMS '17*. https://doi.org/10.1145/3036331.3036349
30. Singh, R., Singh, J., & Singh, R. (2017). Fuzzy based advanced hybrid intrusion detection system to detect malicious nodes in wireless sensor networks. In *Wireless communications and mobile computing, 2017*.