Journal of Computer & Robotics 16(2), Summer and Autumn 2023, 19-35

Fuzzy Clustering Algorithm to Identify Sybil Attacks in Vehicular ad Hoc Networks

Mehdi Maleknasab Ardakani [a], Mohammad Ali Tabarzad [a,*], Mohammad Amin Shayegan[a]

Department of Computer Engineering, Shiraz Branch, Islamic Azad University, Shiraz, Iran

Received 07 February 2023; Accepted 14 March 2023

Abstract

Due to the increasing use of VANET networks and the use of smart systems in these types of networks, their challenges have been the focus of researchers. One of the important challenges of such networks is the security issues that threaten this category of networks. In this article, the Sybil attack, which is one of the security challenges in VANET networks, has been investigated and identified. In a Sybil attack, a node threatens VANET networks by stealing the identity of other nodes or creating a virtual identity, by making incorrect decisions and sending false information. In this article, the clustering method is used to avoid the overhead of identification nodes in centralized methods and avoid delay in distributed methods. RSU determines the cluster head with the help of fuzzy logic. The cluster head creates moving clusters by placing similar nodes in terms of direction, speed, and distance in separate clusters while moving. The cluster head performs malicious node detection using a directional antenna and a fuzzy system. The first fuzzy system places the cluster head in the best possible place of the cluster. The cluster head identifies the malicious nodes in each cluster locally, while the second fuzzy system interferes in determining the validity of the cluster members. In the proposed plan, in addition to optimizing the sending and receiving of messages, The simulation results show that the proposed method has improved by 1.2% in detecting the malicious node, 0.4% in the number of false positive detection, 0.6% in the lost packet, and 0.1% in the delay compared to the previous methods.

Keywords: VANET, Sybil attack, fuzzy logic, clustering, directional antenna

1.Introduction

Intelligent Transportation Systems (ITC) were created to improve the safety, security, and efficiency of public transportation networks. The Vehicular ad hoc network (VANET) is a part of intelligent transportation systems that aim to implement information technologies in vehicles and transportation infrastructure. There are three types of communication in these networks, which are vehicle-to-vehicle communication, which is called (V2V). The connection of the vehicle with the roadside station unit (RSU), which is called (V2R), and the connection of the roadside stations with each other, which is called (R2R), all of them together form the VANET network.

VANET networks are classified as an application of mobile networks. These networks create wireless communication between moving vehicles by using dedicated short-range communication (DSRC). It is a version of IEEE802.11a that has been improved for operation with low overhead in the form of IEEE802.11p standard.

By using technologies such as dedicated short-range communication and by exchanging sensitive information such as the position, speed, and direction of movement of cars up to a certain range, drivers of cars equipped with this technology have a higher level of awareness regarding the presence of other cars near them and can Receive timely information, make informed decisions to deal with

[*] Corresponding Author. Email: tabarzad@iaushiraz.ac.ir

dangerous situations and avoid getting into accident-causing situations. In addition to critical safety applications, this technology can bring about an important transformation in mobility and traffic smoothing [3]. Also, having enough information, drivers will be able to choose better routes and modify their driving patterns, which will result in reduced fuel consumption and more environmentally friendly driving. These networks have many challenges because they have limited bandwidth and dynamic topology. One of these challenges is the security of VANET networks. The misbehavior of some cars in communication and routing protocols causes the network to fail, so misbehaving cars should be identified in the shortest possible time and prevent improper operation. In this way, car networks can be protected against such damages [1].

Many attacks through malicious nodes threaten VANET networks. These networks are affected by various types of attacks, one of which is the Sybil attack. Sybil attacks can be easily implemented in VANET networks because VANET nodes are located in a distributed environment and communicate with each other through radio waves. This same feature provides the possibility for an attacker to attack the network.

Sybil attacks are considered a serious threat to VANET networks. In such attacks, a malicious node creates several fake identities for itself and misleads network nodes. These attacks can interfere with operations such as routing, voting, data aggregation, evaluation of nodes' credibility, fair resource allocation, and misbehavior detection. Mechanisms that are based on voting lose their efficiency because some nodes are fake and the information obtained from them cannot be trusted [2].

Information security is very important in some systems. For example, the confidentiality and security of information are very important where nodes transmit critical information or routing activities. Sybil attacks are therefore one of the most important attacks in VANET networks, which can provide the necessary platform for many other attacks [2]. Also, this attack targets traffic control and causes extensive damage to the network.

Considering the simplicity of implementing these attacks and the sensitivity of the information in these types of networks, it is very necessary to provide solutions that can detect Sybil attacks and deal with them if possible. These solutions should take into account the dynamism of the VANET networks and the rapid change of its topology to be practically usable in these networks.

So far, many methods have been proposed to deal with or detect such attacks. For example, some researchers have been introduced with the help of information received from neighbors, some with the help of encryption, and some with the help of path tracking, each of which has characteristics and disadvantages, but researchers are still trying to obtain newer methods that cover all purposes. In this article, the method of identifying Sybil security attacks with the help of moving clusters and using cluster heads calculated by fuzzy method and the use of a directional antenna is presented.

In the proposed method, the idea that vehicles on high-traffic roads are usually moving together in a group has been used, and to create this group, cluster heads are determined, which have the task of identifying and removing vandal nodes. RSUs determine cluster heads with the help of fuzzy systems and select the node that is in the best position to form the cluster.

Fuzzy systems can estimate the best possible state from several different parameters. In such systems, several parameters are given as input to the fuzzy system, each of these parameters is a feature that describes the desired object and has an output that is obtained from the commonality of the inputs with the help of fuzzy rules.

In this article, the feature of speed, position relative to neighboring nodes, and the number of neighboring nodes of moving vehicles are determined as inputs to the fuzzy system, and the output value is calculated for each node. The node with the most neighbors and the smallest distance from the neighbors and the smallest speed difference has the largest output value and is selected as the cluster head.

Along the way, this cluster head calculates the position of the nodes by checking the messages and calculating the direction of the received message and compares it with the position in the message, and if there is a difference, the sending node is introduced as a suspicious and also checks the validity of the sending node with the help of a fuzzy system. If approved, allows joining the cluster and communicating with the cluster members.

Suspicious nodes are labeled by the cluster head and while introducing them to the cluster members, it introduces them to the RSU for final confirmation and removal. This detection and countermeasure method can have many characteristics, such as 1- the detection is performed in all situations, even in places where the RSU is not available 2- since the detection happens locally; the message overhead in the network is significantly reduced. 3- Due to the proximity of the investigated node, with the help of directional antennas, the claimed positions can be confirmed or rejected easily with the cluster head. 4- The time from the beginning of the attack to the time of identifying the attacker is greatly reduced. 5- The accuracy of identification in busy and quiet traffic is improved.

This article has been implemented with the help of MATLAB simulator and the results have been compared with Lim2020, footprint, and maleknasab2022 methods.
The comparison of the results shows that in the proposed scheme, the parameters of attack detection time, message overhead, and the number of false detections have been significantly improved.

The continuation of the article is as follows. In the second part, an overview of the previous methods of identifying Sybil's attack is described. In the third part, the Sybil attack model has been examined. In the fourth section, the objectives of the plan stated in the fifth section are presented in full, and in the sixth section, the simulation and comparison of the proposed method with the lim2020, footprint, and maleknasab2022 methods are stated, and in the seventh section, the conclusions and suggestions for future work are stated.

2. Related Works

Many articles have been written about identifying and preventing Sybil attacks in VANET, each of which has provided a solution to this problem, but in general, they can be divided into the following groups:

2.1. Resource Testing Methods

This method uses this property of a node that cannot be transmitted data simultaneously over more than one channel in a public network. The way it works is that the node that wants to perform the checking action first sends a message to all the members in its neighbor list through dedicated channels. It then waits for a certain time through the same dedicated channels, failure to respond at the specified time means that the node is suspicious. Because the mobility of VANET networks is very high, a response at the specified time is not guaranteed at all, and these methods are not suitable for VANET networks, and on the other hand, there is a high density of nodes [3].

2.2. Methods Based on Received Signal Strength

In these methods, the node calculates the signal strength received when receiving a message from a new sender. Stores the strength of the received signal along with the sender ID in a search table. If in the future, one receives another message with the same signal strength as the previous message but the sender identifier was different, it announces the occurrence of a Sybil attack [4] [5] [6].
Due to the high mobility, the received signal strength is constantly changing, and on the other hand, nodes in Vent networks can change their transmitted power, so these methods also have many challenges.

2.3. Methods Based on Information Received from Nodes

In this method, the node's identity is obtained by analyzing the information of neighboring nodes. In Sybil attacks, forged nodes have a similar set of neighbors.
In [8], the authors reviewed the list of neighbors of each roadside station and stated that if a pair of identical identifiers was observed at similar locations, they would most likely be Sybil nodes. They are based on the two principles that seeing a pair of cars together at the same time in one place means that they are related, and seeing a pair of cars in different places at the same time means that they are not related. They have designed an algorithm that can predict, prevent and neutralize Sybil attacks. In [7], the P2 DAP scheme transmits a report of all events to the RSU to detect a Sybil attack. RSU examines the signatures of each message, considering a single event signed by two different aliases of a vehicle, that vehicle is considered an attacker. In cases where suspicious vehicles need to be verified as a Sybil attackers, the information is sent to the DMV. The DMV uses the HASH

function to obtain the alias of the vehicle that was previously by him Hashed and, by comparing it in the table, identifies the suspicious node.

2.4. Methods Based on Cryptography and Authentication

Encryption and authentication methods are divided into symmetric and asymmetric groups. In asymmetric encryption methods, first public and private keys are distributed among all network nodes, and then a digital signature is generated.

In symmetric encryption, each node has a unique key with RSU. Whenever two nodes have information to exchange, they first contact the RSU and express their desire to communicate. The RSU verifies the identity of the two nodes through their symmetric keys and then sends a common key to both. So that they can communicate directly with each other.

In [10] each node must first be registered by the Trusted Authority and the couple must receive their public and private keys as well as their identification number. The RSU then creates a short-term temporary identity after receiving the original identity and confirming it for the node that entered the domain.

Vehicles use the temporary identity provided by RSU to communicate with other vehicles, with each vehicle compiling a list of neighborhoods based on bacon packages. Then, by sharing the neighborhood list after each interval, the vehicle checks the subscription of all neighborhood lists after 4 to 5-time intervals. If some nodes are constantly seen in a vehicle's neighborhood, these nodes may be Sybil nodes.

In [11], each vehicle is registered separately with the Road and Transportation Administration. Vehicle nicknames are generated with the help of RSUs. An identity-based encryption approach is implemented to sign messages. Each vehicle must receive one or more token signs when registering. Otherwise, the vehicle will not be able to access communication services within that particular area. Thus, the level of anonymity is directly proportional to the number of nicknames.

This plan has been implemented in three phases. In the first phase, the Trusted Authority (TA) creates the security parameters for each of the vehicles and the RSU. These parameters are used to prepare the data integrity signature and verify the proposed authentication method. In the second phase, each vehicle and RSU must contact a TA to set up security issues and the group authentication process on a confidential channel. In the third phase, each vehicle calculates its validation code to verify the message during the VANET communication process.

The disadvantages of cryptographic methods in VANET networks are the lack of a secure channel for key distribution and also the lack of a valid reference to confirm or reject suspicious nodes.

2.5. Position-Based Methods

In these methods, the position of the nodes is usually confirmed or rejected by other nodes or the RSU. In the footprint algorithm [12], when a vehicle encounters RSU roadside radios, at the request of that vehicle, the roadside radios for this vehicle send an authorized message to prove its presence and time in The range of these roadside radios. The message generated by the RSU is sent to the requesting node and the surrounding RSUs. The authorized message series can then be used directly to identify vehicles.

2.6. Smart Methods

One of the methods that have been considered in recent years to detect Sybil attacks in VANET is the use of intelligent algorithms. In these designs, malicious nodes are identified by analyzing the data. [12] A Sybil attacks detection scheme is proposed using Advanced Driver Assistance Systems (ADAS) sensors installed on modern passenger vehicles, without the assistance of a third-party verification authority and infrastructure. A vehicle equipped with ADAS sensors scans the surrounding area and detects nearby objects. In the presence of counterfeit vehicles created by a Sybil attack, the vehicle verifies the alleged location of the vehicle as being authentic or counterfeit. [13] The paper combines the support vector machine algorithm, artificial neural networks, and the AODV protocol with the help of feature node extraction to detect malicious nodes in the VANET network.

Table 1
Comparison of proposals to counter Sybil attacks

Author Name	Year of publication	description	Result
Lim	2020	Vehicles with the help of ADAS sensors scan the surrounding areas and identify the attacking node	Nearby attacker vehicles are detected with an accuracy of over 98% and this detection decreases as vehicles move away.
chang	2012	Nodes receive a message confirming attendance and time as soon as they reach the RSUs, and of series authorized to receive messages is used to identify vehicles.	The footprint algorithm greatly limits Sybil attacks and reduces the impact of Sybil attacks in urban areas (above 98% tracking).
Feng, et al	2019	A local license with two validity and reliability values is given by each RSU to each vehicle if the validity and trust value of the event is below the corresponding threshold values when sending the message. The message is stopped and the sender node is detected as a Sybil attacker.	The latency of the proposed method is about 4 milliseconds less than previous methods. The package delivery ratio has improved by an average of about 0.4% compared to previous methods
Dutt &Joshi	2019	To strengthen the detection of Sybil attacks, they strengthened the EBRS method by securing RSU and TA. They compared hash values instead of reputation values because reputation may be violated in certain cases. To validate events and nodes, in this system RSUs have events with a hash value for those who use this particular event, to create. By detecting false or fake events that are done by the attacker, the Sybil node makes a diagnosis	The proposed method has reduced packet latency compared to previous methods such as TSA. The package delivery ratio is also improved compared to previous methods
Shaik & Hussain,	2018	An identity-based encryption approach is implemented to sign messages. Each vehicle must receive one or more token signs when registering. And will not be able to access communication services within that range without these tokens. Thus, the level of anonymity is directly proportional to the number of nicknames.	The results show that the detection of Sybil attacks is about 3% and the correct accuracy received of packets is about 0.03 The percentage has improved compared to previous methods...
Girija & Saravanan,	2017	The main idea of this work is to evaluate the similarity of the driving pattern of vehicles, destructive nodes avoid situations that are detected by normal vehicles, and their driving patterns become erratic, especially in dynamic traffic environments.	Compared to previous methods, this idea has reduced the delay time in detecting Sybil attacks by 30%, increased the detection rate of Sybil attacks by 15%, and controlled the frequency of generating attack nodes by up to 40%.
Panchal & Singh,	2017	First, a random value between one and zero is given to each node. Then, with the help of the initial energy of the signal and the final energy of the message signal, as well as the number of nodes traveled and the number of packets sent, the value of trust is obtained. Each node calculates the value of the credit as soon as it receives the packet and compares it with the threshold value. If the value obtained is greater than the threshold, it is a Sybil node; if this value is less than the threshold, the node is normal.	Compared to the EBRS algorithm, the number of correctly received packets has increased by about 3 tenths of a percent, the detection of Sybil nodes has increased by 4 tenths of a percent, and the packet received latency has improved by an average of 12.5 percent.
Sharma et al.	2017	In this model, the technique of generating dynamic certificates is used to limit the Sybil attack and neighboring information is used to detect the cyber node. Each vehicle compiles a neighborhood list based on bacon packages. Then, by sharing the neighborhood list in each interval, the vehicle checks the subscription of all neighborhood lists after 4 to 5-time intervals. If some nodes are constantly seen in a vehicle's neighborhood, these nodes may be Sybil nodes.	In this article, the only improvement that has occurred is the use of a temporary identity, in Bacon's message, for communication between nodes, which ensures that personal information is protected when communicating between nodes.
Baza et al.,	2019	Each roadside unit (RSU) issues a time-stamped label to prove the vehicle's anonymous location. Which is a combination of the show time and the nickname of the location of this station next to the roads?	Reduces the detection rate of correct nodes that are detected as malicious by about 15% compared to the footprint

		As the vehicle moves, its path is created by combining a set of re-timed approved tags that are temporarily interconnected. This route is used as an anonymous vehicle identity.	algorithm. Also, the detection rate of malicious nodes that are correctly detected has decreased and the detection rate of correct, compared to footprint and has increased up to 40%.
Kumar et al.,	2019	In this paper, by combining support vector machine algorithm, artificial neural networks, and AODV protocol by extracting features from the node, it has been used to detect malicious nodes in the VANET network.	Routing, transmission power, and lost packets are improved

3. Attack Model

Sybil attacks are started by malicious nodes with impersonation to attack neighboring nodes. Network layers and application layers are damaged by Sybil attacks with more activities in using channel resources. A malicious node uses different aliases to generate virtual nodes for the Sybil attack process. The Sybil attack is started by an attacker who has managed to fake or steal one or more identifiers, for example, in Figure 1; the black vehicle sends false messages to neighbors by creating three fake identities with fake positions. with the assertion, the presence of vehicles in those places other vehicles fall into error.

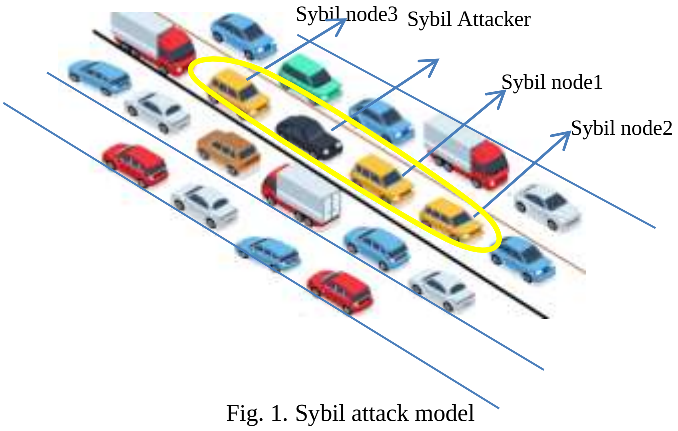

Fig. 1. Sybil attack model

The generated fake situations cause normal nodes to make mistakes in choosing the route, for example, they consider quiet traffic routes as high traffic routes, or in voting, the attacker changes the result in his favor with the fake ballot he created. It also uses fake IDs in other attacks, such as DOS, to implement its own attack goals.

The following points can be mentioned to recognize fake generated IDs.

a. The spoofed ID is for a vehicle that does not currently exist in the range, or the spoofed ID is for no vehicle at all.

b. The claimed location does not exist in this range, or there is no node in that location, or the ID of the node in that location is different from the ID in the message.

c. The speed introduced in the message is out of the speed range defined for common nodes, or the distance traveled in a certain period is not consistent with the stated speed.

d. The movement diagram of the fake node is very different from the normal nodes.

4. Proposed Method

In this article, to identify and prevent this type of attack, the principle of clustering and moving similar nodes together in highways and high-traffic routes are used for local search and reducing the sending and receiving of messages, as well as accelerating the recognition. A fuzzy system is used as follows to determine the cluster head by RSU.

Step1: real value input and conversion to fuzzy

The first step in the fuzzy decision-making process is to reconstruct the real variables; That is, at this stage, the real variables become linguistic variables. The three parameters of the distance between the vehicle and the neighboring vehicles, the number of nodes around the vehicle, and the speed difference between the vehicle and the neighboring vehicles are used as the input of a fuzzy system. These values are all converted to values between zero and one to determine their membership ratio.

Step 2: Check the law:

Based on the previously obtained fuzzy values, the elicitation of these values is determined to specify the new fuzzy output set. With the help of if-then rules, the behavior of the system is determined. For example, a vehicle that has a small speed difference from the rest and a small distance difference from other vehicles, and a large number of nodes that have a direct connection with that node, this node is the most suitable node to become a cluster head.

Table 2 shows the set of rules used in this fuzzy system.

Table 1
Fuzzy rules for cluster head selection

Rule #	Input parameters			Output parameter
	number of surrounding vehicles	distance difference	speed difference	probability of cluster head
1	high	high	high	medium
2	high	high	medium	medium
3	high	high	low	high
4	high	medium	high	low
5	high	medium	medium	medium
6	high	medium	low	high
7	high	low	high	high
8	high	low	medium	high
9	high	low	low	high
10	low	high	high	low
11	low	high	medium	low
12	low	high	low	low
13	low	medium	high	low
14	low	medium	medium	medium
15	low	medium	low	high
16	low	low	high	low
17	low	low	medium	medium
18	low	low	low	high
19	medium	high	high	low
20	medium	high	medium	low
21	medium	high	low	medium
22	medium	medium	high	medium
23	medium	medium	medium	medium
24	medium	medium	low	medium
25	medium	low	high	medium
26	medium	low	medium	medium
27	medium	low	low	high

Step 3- In this step, the fuzzy output is specified for each vehicle

Step 4 In this step, the real output of the final fuzzy system is determined for each of the vehicles.

The fuzzy output value is a real number that determines the rank of each vehicle to be cluster head.

Mamdani method was used to calculate the inferred value. With the help of appropriate fuzzy rules and the Mamdani analysis method, the output of the system has been determined. The output of the fuzzy system is calculated into the components of each of the neighboring nodes of the RSU, and among the obtained values, the node that obtained the largest output value is introduced as the cluster head. Of course, in the proposed method, each RSU must determine both the left-path cluster head and the right-path cluster head.

In this article, directional antennas installed on vehicles and capable of receiving messages by determining the radar angle are used to identify the vandal node, and also a fuzzy system is used to validate the vehicles. As soon as the message is received, its position is checked, and it is confirmed or rejected by checking the positions of the nodes in the cluster, and the reception angle is calculated with the help of the location coordinates of the cluster head and the sender. Then the angle of the antenna and the angle of the message are compared and if there is a discrepancy, the message is suspicious and the sending node is known as Sybil. The cluster head introduces the Sybil node to the cluster members and RSUs to remove it from the network and ignore its messages.

The routing algorithm used to send messages in this article is the AODV routing protocol. Using the AODV routing protocol makes the routes not include loops and the shortest possible route is also selected. Also, this protocol can make manual changes in routes and if there is an error, it will be able to find and replace new routes. The AODV protocol quickly adapts to the dynamic topology conditions of the VENET. Another feature of this protocol is the low amount of processing and memory required. The AODV protocol uses the destination sequence number to prevent loops.

Objectives of the plan

Sybil attack detection scheme in VENT networks should achieve three goals:

1. Privacy: The vehicle does not want to share its information with other vehicles and RSUs because such information can be confidential. The detection scheme should prevent vehicle information leakage.
2. Rapid detection: When a Sybil attack occurs, the detection scheme must react before the attack ends. Otherwise, the attacker can reach his goal.
3. Individual diagnosis: The principle of Sybil's attack is that the decision is made based on group discussions. To eliminate the possibility of starting an attack, the diagnosis should be done independently by the checker without collaboration with others.

assumptions:

- All nodes periodically broadcast the beacon packet
- Each beacon package includes a nickname and position coordinates at the moment of sending the message, timer - speed, direction, etc.
- RSUs are installed in the road area
- The TA authority is responsible for assigning vehicle nicknames and transferring them to nodes and RSUs
- There is a reliable connection between TA references and RSUs
- RSUs and TA are valid
- All vehicles are equipped with an OBU device and directional antenna

In the proposed method, same-direction vehicles are divided into separate clusters, and the task of finding the malicious node is the responsibility of the cluster head and cluster members, as well as the RSU. In addition to determining the cluster head, RSUs are also responsible for identifying the malicious node. For this purpose, as soon as each vehicle enters the area of an RSU, it sends a beacon message to introduce itself, the RSU checks the position of the node with the help of a directional antenna and then Confirms or rejects the node If the node is valid, the RSU stores the vehicle ID to participate in the cluster head determination. The RSU determines the cluster head from among the surrounding vehicles within a certain time; In this paper, this duration is equal to the time a vehicle travels the RSU range with an average speed. Figure 2 shows the flowchart of cluster head selection steps.

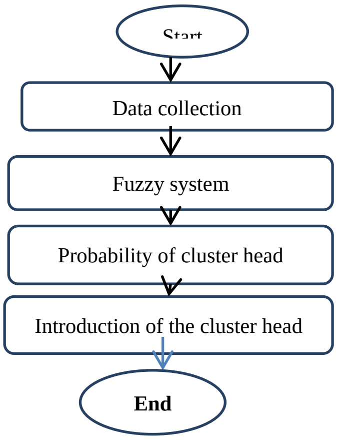

Fig 2: Cluster head selection steps

Figure 3 shows the fuzzy system of cluster head determination, where the inputs and outputs of the trapezoidal membership functions and the Mamdani system are used to analyze the inputs.

The inputs of the fuzzy system are the sum distance difference of the vehicle with the surrounding vehicles ADL, the number of nodes around the vehicle NCL and the sum speed difference of the vehicle with the surrounding vehicles AVL.

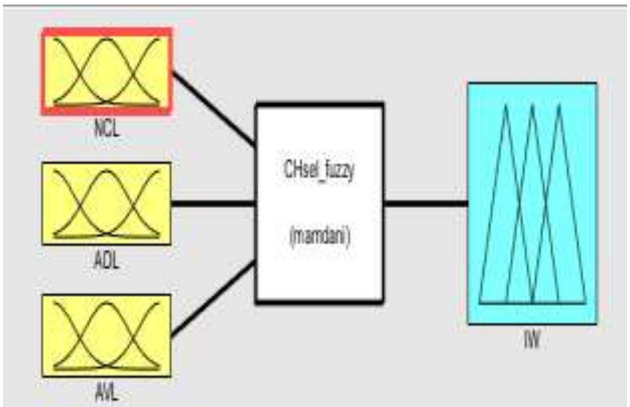

Fig. 3: Fuzzy cluster head selection system

A number of neighboring nodes: RSU counts neighboring nodes of each node (refers to nodes that directly communicate with the node and their distance is less than 300 meters) and assigns to each node the number of neighboring nodes. Equation 1 shows the number of neighboring nodes

$$NCL=n \qquad d_k<300 \qquad (1)$$

d_k is the distance of the node from other nodes and n is the number of nodes whose distance from the desired node is smaller than 300. Figure 4 shows the membership function of neighboring groups, which is trapezoidal-triangular.

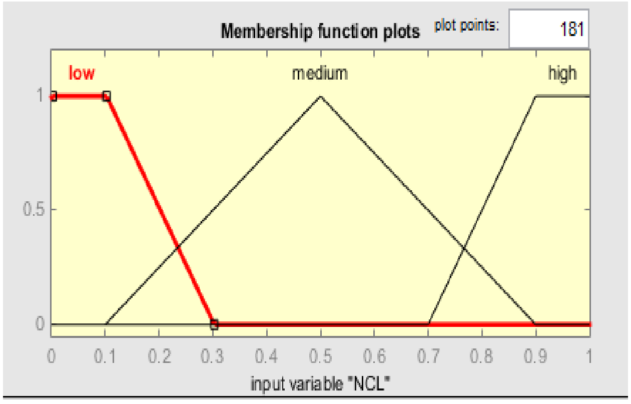

Fig. 4: Membership function of neighboring nodes

Average Distance difference: RSU, using the formula 2[42].

$$d = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \qquad (2)$$

Where (x, y) are the coordinates of the location of the vehicles, it obtains the distance of each node from the others and sums the results, and assigns it to each node as the distance difference (the purpose calculating the distance between each node and other nodes is adjacent to RSU). Formula 3 is used to calculate the average distance difference between each node with other nodes

$$ADl = \frac{\sum_{i=1}^{n}(d_k - d_i)}{n} \qquad (3)$$

Where d is the distance between the nodes, k is the desired node, and n is the number of nodes around the RSU.

Figure 5 shows the membership function of the average distance difference. This function has been selected as trapezoidal-triangular for more accurate performance.

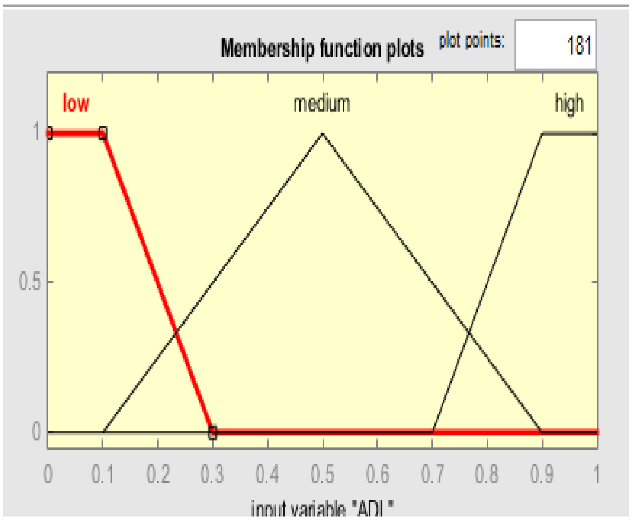

Fig. 5: Distance membership function

Average Speed difference: The speed difference of the node with neighboring nodes is measured by RSU at the moment of cluster head calculation. This speed difference is calculated for all nodes and is used as one of the input parameters for each node in the cluster head selection. (The goal is to calculate the average sum of the speed differences between each node and the other nodes). Equation 4 is used to calculate the average speed difference of each node with other nodes.

$$AVl = \frac{\sum_{i=1}^{n}(v_k - v_i)}{n} \qquad (4)$$

Where v_k is the speed of the target node, v_i is the speed of other neighboring nodes RSU.

Figure 6 shows the membership function of the average distance difference. This function has been selected as trapezoidal-triangular for more accurate performance.

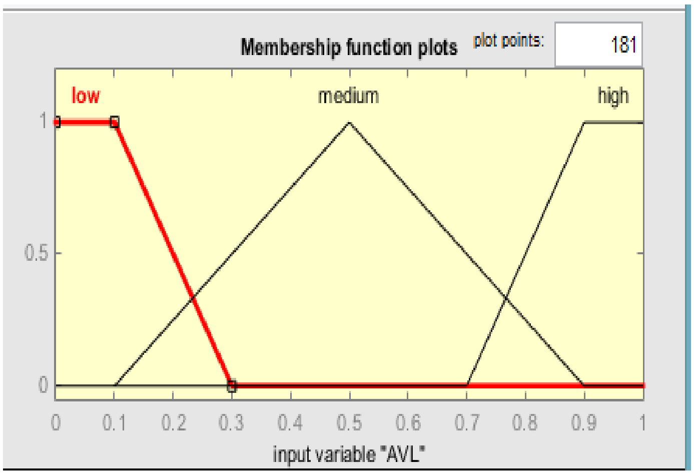

Fig 6: Speed membership function

System output: Finally, each RSU gives the calculated information of its neighboring nodes as input for each node to the fuzzy system, and then the node that has the best state in the output of the fuzzy system is selected as the cluster head. and to other nodes introduce. The steps to select the cluster head are as follows

1) $V_i. ADl = \sum_{i=1}^{n}(d_k - d_i)$
2) $V_i .AVl = \sum_{i=1}^{n}(v_k - v_i)$
3) $NCL = n$
4) V_i.F=fuzzy($V_i. ADl$, Vi. AVl, NCL)
5) Cluster=max(V_i.F)

RSU selects the node that has the most neighbors, the smallest distance difference, and the smallest speed difference as the cluster head. if several nodes have equal chances to be the cluster head, the node with the lowest speed difference is selected.

The output of the fuzzy system is calculated according to the values of the input parameters for each node, and each RSU determines two cluster heads, one for the nodes that move from left to right and the other for the nodes that move from right to left. This value is extracted from the fuzzy set using Equation 5, which uses the Center of Surface (COA) method to obtain the output [41]. In this equation,A (x) represents the membership function of fuzzy sets.

$$COA=\frac{\int_z \mu A(x)zdz}{\int_z \mu A(z)dz} \quad (5)$$

Figure 7 shows the output membership function that has been selected as trapezoidal-triangular

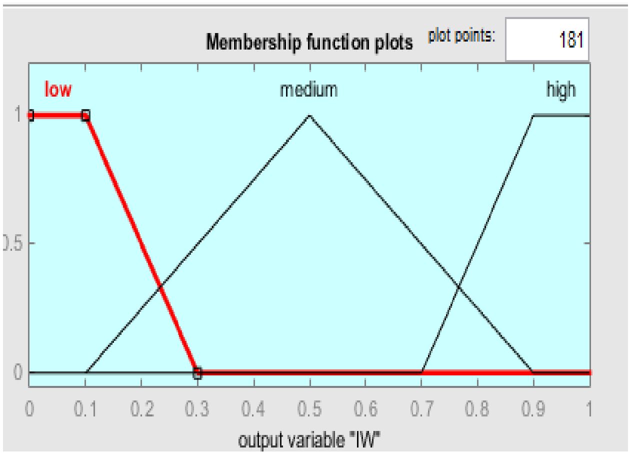

Fig.7 output membership function

After determining the cluster head, the nodes introduce themselves to the surrounding cluster heads by sending a message. Cluster headers check the received message and determine its validity. And if they are valid, they will join the node and they will be allowed to send messages.

Nodes use the beacon received from the cluster head and their locator to confirm the cluster head of their range.

Each cluster head moves along the path with its members. Along the way, some vehicles are removed from the cluster and others are added to the cluster.

If the connection between the node and the cluster head is interrupted, the node again requests membership to the surrounding cluster heads.

Nodes use the AODV algorithm to send messages.

The steps to confirm and join the node in the cluster are as follows:

To identify the malicious node with the help of the directional antenna and the position in the message, the cluster head checks the validity of the claim, if the angle obtained from the directional antenna and the angle calculated using the position in the message are not equal, the claim is not confirmed and the node is introduced as Sybil. The position angle in the message is calculated using the following formula [42].

$$\alpha = \tan^{-1}\frac{y_1-y_2}{x_1-x_2} \quad (6)$$

Where (x_1, y_1) are the coordinates of the cluster head and (x_2, y_2) are the coordinates of the node sending the message.

If the above two angles are equal, the cluster head looks for the node ID in the neighbor list, if it exists, it is allowed to connect, otherwise, the node membership is checked with the help of the fuzzy system. If the node obtains the necessary score in the fuzzy system, it is allowed to communicate. Otherwise, communication is not allowed.

In this article, a fuzzy system is used to determine the membership. This system uses four inputs: velocity difference (VD) with the cluster head, distance difference (DD) with the cluster head, presence time (PT) in the cluster, and received signal strength. Each of the modes can have three modes: low, medium, and high. And with the help of fuzzy rules and Mamdani inference, they are converted into three good, average, and bad output states. The true value of the output expresses the cluster membership score. Figure 8 shows the architecture of the fuzzy membership determination system

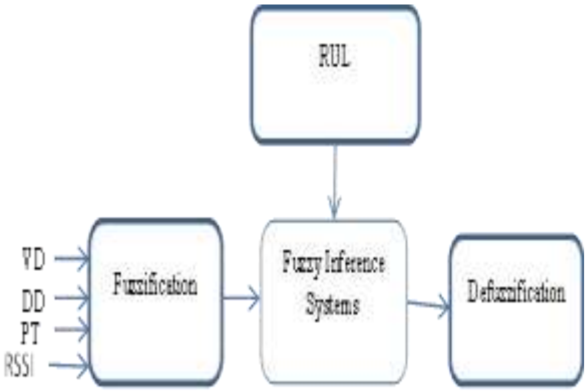

Fig.8 The architecture of the fuzzy membership determination system

The fuzzy membership determination system has three inputs: distance difference and speed difference with the cluster head and the time of being in the cluster. If the output of this numerical fuzzy controller is less than 0.4, the membership of the node is not accepted. But if it is 0.4 or more, its membership is accepted. Triangular membership functions have been used in the inputs and outputs of the fuzzy system, and the analysis of the rules has been done with the help of Mamdani fuzzy system.

Sybil node identification and its membership in the cluster happen at the same time, that is, if the node is valid, it is allowed to join and can send messages, but if the node's validity is not confirmed, it cannot operate in this cluster. Figure 9 shows the flowchart of node identification and membership in the cluster.

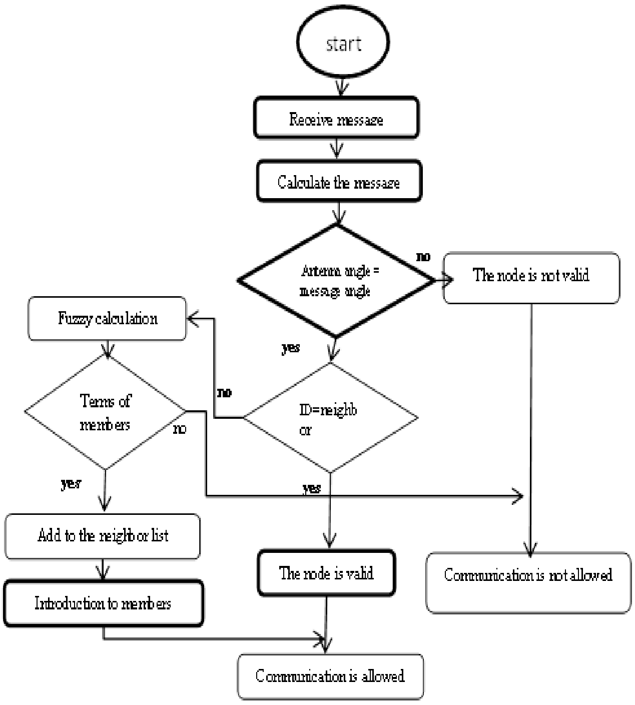

Fig. 9 membership check flowchart

The proposed algorithm detects the Sybil node by determining the cluster locally with the least sending and receiving messages. In addition to reducing the traffic load of the network, this work also makes Sybil node detection faster. The fuzzy system helps to select the cluster members more optimally and establish stronger connections between the cluster head and its members by finding the node with the right position to become the cluster head and also to be a member of the cluster.

5. Simulation

The proposed algorithm with the help of MATLAB software in a 5000-meter highway with three paths went and return with 5 RSUs and with 120 nodes for low traffic and 1250 nodes for high traffic and with four types of Sybil attacks of 5, 10, 15, 20 percent of nodes, with Random coordinates are implemented in the road boundary and random speed of nodes between 20 and 30 m/s assigned to each node. Table 3 shows the simulation parameters.

Table 3
Simulation parameters to evaluate the proposed Sybil attack management scheme

parameter	**value**
simulator	Matlab
Simulation time	500 seconds
Number of vehicles	120 low-traffic, 1250 high traffic
Number of RSUs	5
Car speed	20 to 30 km/s
The number of Sybil	nodes are 5, 10, 15, and 20 percent of all nodes
Mac protocol	IEEE 802.11p
Number of virtual nodes	1-5 IDs randomly per Sybil node
RSSI	0.3
Simulation area	5000×70
routing protocol	AODV(Ad hoc On-Demand Distance Vector)
transport protocol	UDP
RSU radio range	500m
Vehicle radio range	300m
The number of averaging periods	20

First, valid nodes and Sybil are spread randomly on the road surface, and RSUs are placed on the side of the road at a distance of 1000 meters from each other. The range for sending and receiving messages is 500 meters for each RSU and 300 meters for vehicles.

The RSU After receiving the message from the vehicles in its range calculates with the help fuzzy system with input the values of the speed difference, the average distance, the number of neighbors, and the Probability of being the cluster head for each of them.

Each RSU selects a vehicle with the highest output value as the cluster head among its neighboring nodes for each direction. and introduces the members of the cluster, and the nodes that are adjacent and in the same direction as these cluster heads can become members of the cluster and move on the road as a group if they have the necessary score from the fuzzy membership selection system. Nodes periodically introduce themselves to the cluster head and other nodes. Valid nodes send a message including position and identification number and speed to the cluster head in each period. But Sybil nodes, in addition to their introduction message, randomly send one to five other messages with fake information to the cluster head and network.

Upon receiving the message from the nodes, the cluster head checks the position of the nodes and confirms or rejects the message with the help of the directional antenna. If the message is incorrect, it identifies the sending node and introduces it to the nearest RSU. RSU checks and deletes the node, if the message is confirmed in the previous step, its ID is compared with the list of neighbors, if it is in the list, it is allowed to connect, otherwise, with the help of the fuzzy system, the score of the node sending the message is calculated and in If it has the necessary points, it is added to the neighbor list and it is allowed to communicate, otherwise the node is recognized as a Sybil.

The simulation has been done to check the parameters, detection percentage, FPR false detection percentage, delay, and also the lost packet ratio in two types of busy traffic and quiet traffic.

Detection percentage: The average detection percentage of the fake node obtained in 20 simulation cycles. The fake node detection rate for each period is obtained from Equation 7

$$D_R = \frac{DR_d - DR_{fp}}{DR_i} \qquad (7)$$

In Equation 7, D_R is the identification rate of the malicious node, DR_d is the total number of detected Sybil nodes in each period. DR_{fp} is the number of valid nodes as Sybil-identified nodes, and DR_i is the number of Sybil nodes produced in each period.

Fpr: The ratio of the average percentage of false detection is equal to the average percentage of the number of correct nodes that have been wrongly detected as Sybil. The FPR ratio for each period is obtained from formula 8\

$$fpr = \frac{fp}{fp+Tp} \qquad (8)$$

In formula 8, fp represents the number of correct nodes that are detected as false, and Tp represents the number of fake nodes that are detected correctly.

Lost packet ratio: The average percentage of the lost packet is equal to the average percentage of the number of unreceived messages 20 times running the simulation program. The lost packet ratio for each period is obtained from relationship 9

$$LP = \frac{\mathrm{SP}-\mathrm{RP}}{\mathrm{SP}} \qquad (9)$$

In relation 9: LP represents the ratio of the number of lost packets, SP, the number of sent packets, and RP, the number of received packets in each period.

Delay: Delay can be defined as the time engaged aimed at a packet to be communicated diagonally to the network from one node to another destination node.

The simulation results based on the graphs below show that the detection percentage is improved compared to maleknasab2022 [41], Lim2020 [1], and Footprint [18] algorithms, and due to the local detection, the false detection percentage is also reduced, and on the other hand, the detection time is significantly reduced.

Figure 10 examines the detection graph of Sybil nodes in the network with high traffic for four types of attacks. Each type of attack has been repeated 20 times, and the value of the graph represents the average detection of the Sybil node in these 20 times. As shown in this figure, the proposed method performs better in any type of attack. With the increase in the number of attackers, the resistance of the proposed plan is higher than other methods in recognizing the Sybil node.

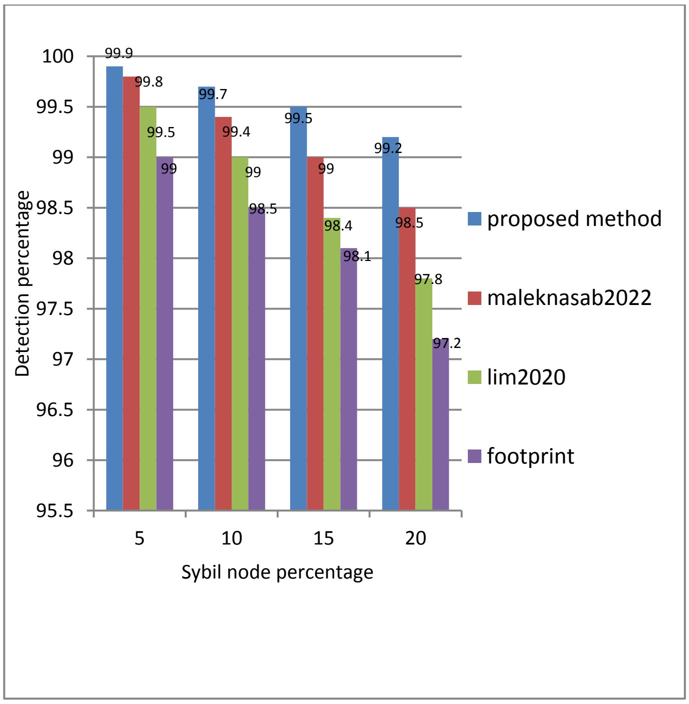

Fig.10 Identifying Sybil in a network with high traffic

Figure 13 shows the detection graph of Sybil nodes for four types of attacks with low traffic. The average Sybil node detection for each period shows that the proposed method compared to the other two methods, in addition to performing better in each period, also has better stability against the increase in the number of Sybil nodes. Also, comparing the graph of Figure 11 and Figure 13 shows that the proposed method performs better in high-traffic environments.

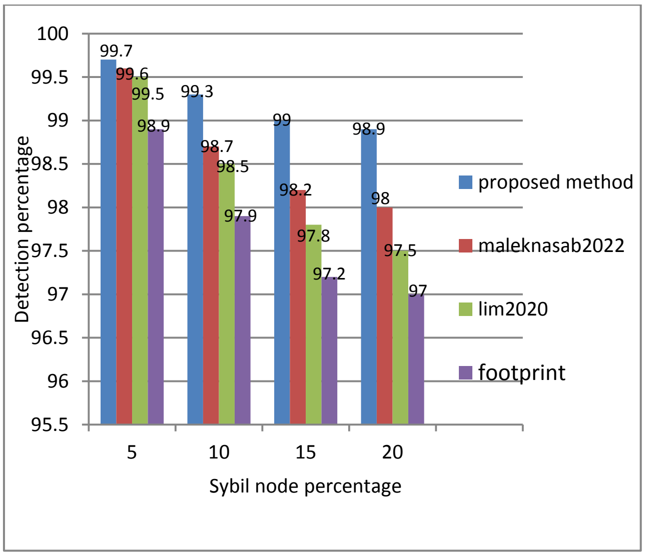

Fig .11 Sybil node identification diagram in VANET with low traffic

Figure 12 shows the graph of FPR false detection percentage for four types of attacks with high traffic. The average FPR for each period shows that the proposed method compared to the other two methods, in addition to having a better performance, there are very few changes in the average FPR with the increase in the number of Sybil nodes.

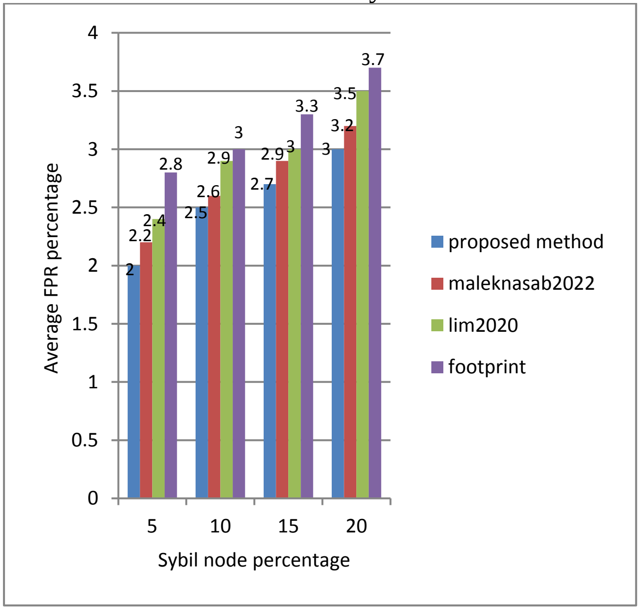

Fig. 12 A comparison chart of FPR in heavy traffic

Figure 13 shows the graph of FPR false detection percentage for four types of attacks with low traffic. The average FPR for each period shows that the proposed method compared to the other two methods, in addition to having a better performance, there are very few changes in the average FPR with the increase in the number of Sybil nodes.

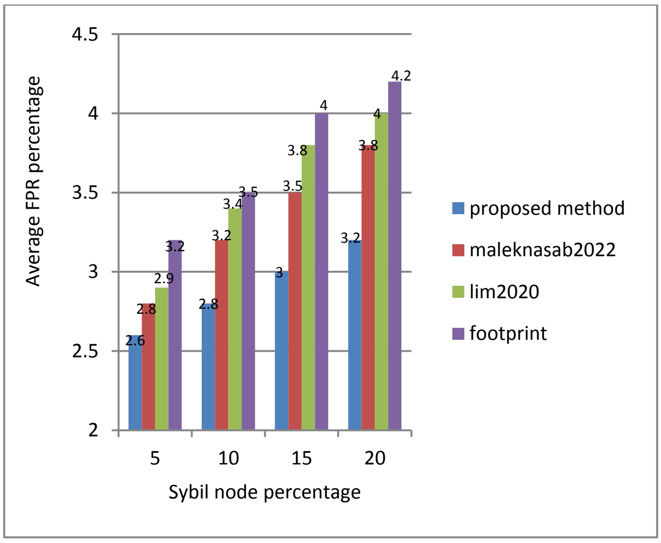

Fig.13: Comparative chart of FPR in low traffic

Figure 14 shows the lost packet ratio graph for four types of attacks with high traffic. As the graph shows, the ratio of missing packets in the proposed method in each period separately and in the average of all periods is less than the other two methods, which indicates an improvement in the performance of the proposed method.

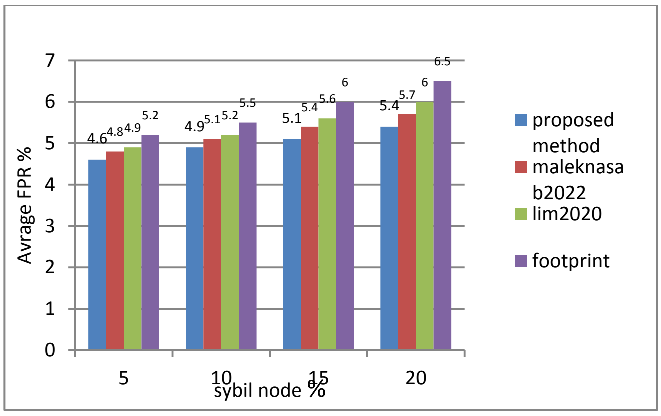

Fig.14 Comparative chart of lost packet ratio in heavy traffic

Figure 15 shows the graph of the lost packet ratio for four types of low-traffic attacks. As the graph shows, the ratio of missing packets in the proposed method in each period separately and in the average of all periods is less than the other two methods, which indicates the better performance of the method. Comparison of Figures 17 and 18 shows that the proposed scheme has a higher percentage of lost packets in quiet traffic areas. The reason is that the nodes could not find a cluster head in the network with low traffic, and on the other hand, due to having fewer neighbors, fewer packets have reached the destination.

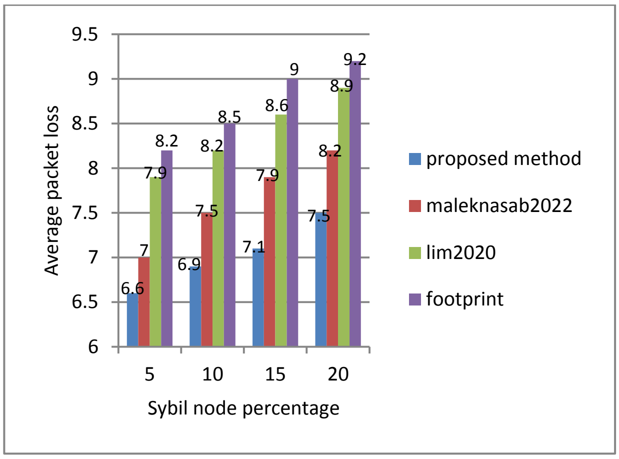

Fig. 15: A comparison chart of the lost packet ratio in low traffic

Figure 16 shows the packet delay comparison diagram. This diagram is related to the time it takes for a packet to reach its destination. The diagram shows that the proposed plan has been able to improve the obstacles such as detection time, the route of the package to the destination, and the routing performance by using clustering and reducing the delay of the package to the destination.

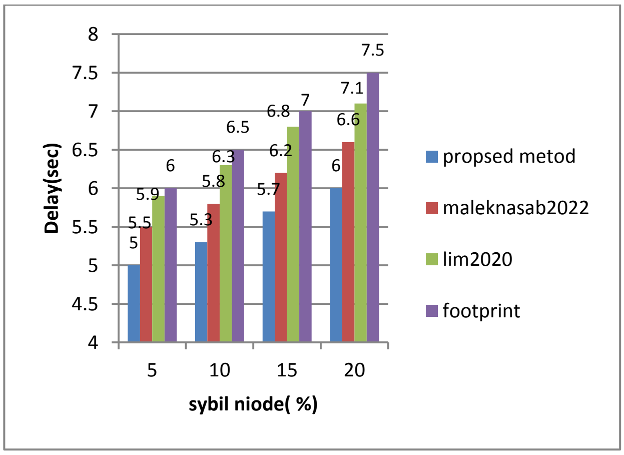

Fig.16 Comparative chart of delay in heavy traffic

Figure 17 shows the comparison chart of packet delay in low traffic. This graph shows that in low traffic, due to the high speed of vehicles and the low number of neighboring nodes, the delay in receiving packets is higher. In this comparison, the proposed method was able to improve the delay of receiving packets compared to other methods due to the clustering and connection of nodes with the cluster head and quick removal of Sybil nodes.

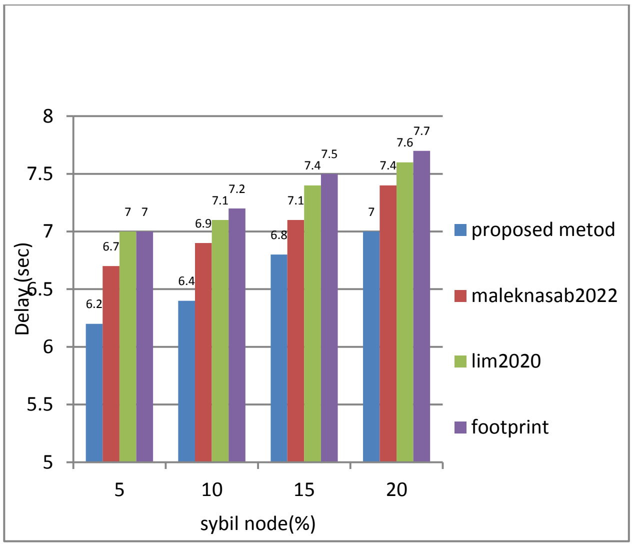

Fig.17 Comparative chart of delay in heavy traffic

As the simulation results show, with the increase of Sybil nodes, the proposed method performs better in the experiments. In the worst case scenario, when the number of Cybil nodes reaches 20% of the total nodes, compared to when the number of Cybil nodes is 5% of the total nodes, the packet receiving delay is only 0.8 seconds, the percentage of lost packets is 1.1%, and the detection percentage is 1%. Finds. Therefore, the proposed method has a good capability in more attacks than other methods.

Tables 4 and 5 and 6 show the summary of the simulation performance. As the table shows, in all cases, the proposed method has better performance, but in crowded traffic, the ratio of this superiority is higher, which indicates that the proposed method is more efficient in crowded traffic.

Table 4
Comparison of the performance of the proposed method with other methods (FPR calculation)

Proposed model	Maleknasab2022	Lim2020	Footprint	Sybil node percentage	Traffic type
2.6	2.8	2.9	3.2	5	heavy traffic
2.8	3.2	3.4	3.5	10	
3	3.5	3.8	4	15	
3.2	3.8	4	4.2	20	
2	2.8	2.4	2.8	5	Light traffic
2.5	3.2	2.9	3	10	
2.6	3.5	3	3.3	15	
3	3.8	3.5	3.7	20	

Table 5
Performance comparison of the proposed method with other methods (lost packet ratio)

Proposed model	Maleknasab2022	Lim202	Footprint	Sybil node percentage	Traffic type
6.6	7	7.9	8.2	5	Light traffic
6.9	7.5	8.2	8.5	10	
7.1	7.9	8.6	9	15	
7.5	8.2	8.9	9.2	20	
4.6	4.8	4.9	5.2	5	heavy traffic
4.9	5.1	5.2	5.5	10	
5.1	5.4	5.6	6	15	
5.4	5.7	6	6.5	20	

Table 6
Performance comparison of the proposed method with other methods (delay)

Proposed model	Maleknasab2022	Lim2020	Footprint	Sybil node percentage	Traffic type
5	5.5	5.9	6	5	heavy traffic
5.3	6.3	6.3	6.5	10	
5.7	6.8	6.8	7	15	
6	7.1	7.1	7.6	20	
6.2	6.7	7	7	5	Light traffic
6.4	6.9	7.1	7.2	10	
6.8	7.1	7.4	7.5	15	
7	7.4	7.6	7.7	20	

6. Conclusion

In this article, fuzzy clustering and directional antenna as well as a fuzzy controller to determine cluster membership were used to protect VANET networks.In the proposed plan, with the help of the directional antenna in the RSU and the cluster head, Sybil's attack was detected in the clusters and around the RSU. The proposed scheme increased the security in this group of networks by increasing the detection level of the malicious node and shortening the detection time. Also, by performing local detection operations and preventing the sending of messages by nodes that are not members of the group, it prevented Sybil attacks from members outside the cluster. With this method, sending many messages to the entire network and increasing network traffic was prevented. The proposed scheme has an average improvement of 0.4 in FPR and 0.6 in lost packet ratio.

In the future, to identify malicious activities, intelligent methods can be used to learn the optimal choice of fuzzy rules for each environment. Also, the proposed plan will be examined for different scenarios with different attacker models, to improve the performance and further evaluate the plan.

References

[1] Malhi, A. K., Batra, S., & Pannu, H. S. (2020). Security of vehicular ad-hoc networks: A comprehensive survey. Computers and Security, 89, 101664. https://doi.org/10.1016/j.cose.2019.101664

[2]

[3] Hammi, B., Idir, Y. M., Zeadally, S., Khatoun, R., & Nebhen, J. (2022). Is It really Easy to Detect Sybil Attacks in C-ITS Environments: A Position Paper. IEEE Transactions on Intelligent Transportation Systems, PP, 1–15. https://doi.org/10.1109/TITS.2022.3165513

[4] Douceur, J. R. (2002). The Sybil attack. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2429, 251–260.

[5] Yao, Y., Xiao, B., Wu, G., Liu, X., Yu, Z., Zhang, K., & Zhou, X. (2017). Voiceprint: A Novel Sybil Attack Detection Method Based on RSSI for VANETs. Proceedings - 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2017, 591–602

[6] Sefati, S. S., & Tabrizi, S. G. (2022). Detecting Sybil Attack in Vehicular Ad-hoc Networks (Vanets) by Using Fitness Function, Signal Strength Index, and Throughput. Wireless Personal Communications, 123(3), 2699–2719. https://doi.org/10.1007/s11277-021-09261-x.

[7] Bouassida, M. S., Guette, G., Shawky, M., & Ducourthial, B. (2009). Sybil Nodes Detection Based on Received Signal Strength Variations within VANET Geometrical Analysis of Sybil. *International Journal of Network Security*, *9*(1), 22–33.

[8] Yao, Y., Xiao, B., Yang, G., Hu, Y., Wang, L.,& Zhou, X. (2019). Power Control Identification: A Novel Sybil Attack Detection Scheme in VANETs Using RSSI. *IEEE Journal on Selected Areas in Communications*, *37*(11), 2588–2602.

[9] Hamed, H., Keshavarz-Haddad, A., & Haghighi, S. G. (2018). Sybil Attack Detection in Urban VANETs Based on RSU Support. *26th Iranian Conference on Electrical Engineering, ICEE 2018*, 602–606.

[10] Zhou, T., Choudhury, R. R., Ning, P., & Chakrabarty, K. (2011). P2DAP - Sybil attacks detection in vehicular ad hoc networks. IEEE Journal on Selected Areas in Communications, 29(3), 582–594

[11] Zhou, T., Choudhury, R. R., Ning, P., & Chakrabarty, K. (2011). P2DAP - Sybil attacks detection in vehicular ad hoc networks. *IEEE Journal on Selected Areas in Communications*, *29*(3), 582–594

[12] Azees, M., Vijayakumar, P., & Deborah, L. J. (2017). EAAP: Efficient Anonymous Authentication with Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks. IEEE Transactions on Intelligent Transportation Systems, 18(9), 2467–2476.

[13] Balaram, A., & Pushpa, S. (2018). Sybil attack resistant location privacy in VANET. International Journal of Information and Communication Technology, 13(4), 389–406

[14] Grover, J., Laxmi, V., & Gaur, M. S. (2014). Sybil attack detection in VANET using neighboring vehicles. International Journal of Security and Networks, 9(4), 222–233

[15] Chang, S., Qi, Y., Zhu, H., Zhao, J., & Shen, X. (2012). Footprint: Detecting Sybil attacks in urban vehicular networks. IEEE Transactions on Parallel and Distributed Systems, 23(6), 1103–1114

[16] Lim, K., Islam, T., Kim, H., & Joung, J. (2020). A Sybil Attack Detection Scheme based on ADAS Sensors for Vehicular Networks. 2020 IEEE 17th Annual Consumer Communications and Networking Conference, CCNC 2020, 1–5.

[17] K. Lim and K. M. Tula Dhār, “LIDAR: Lidar information based dynamic v2v authentication for roadside infrastructure-less vehicular networks,” in Proceedings of the 16th IEEE Annual Consumer Communications & Networking Conference, 2019, pp. 1–6.

[18] Karimi, M. R., & Sadeghi, R. (2021). Improvement of Sybil Attack Detection in Vehicular Ad-Hoc Networks using Cross-layer and Fuzzy Logic. Majlesi Journal of Electrical Engineering, 15(1), 9–18.

[19] Shaik, K., & Hussain, M. A. (2018). Broadcast message authentication mechanism to detect clone and Sybil attacks in VANET’s based on ID-Based signature scheme. International Journal of Engineering and Technology(UAE), 7(3.12 Special Issue 12), 1102–1111.

[20] Abdulkader, Z. A., Abdullah, A., Abdullah, T., & Zukarnain, Z. A. (2018). A Survey on Sybil Attack Detection in Vehicular Ad hoc Networks (VANET). Journal of Computers, 29(2), 1–6.

[21] Aleena Ann Jose1, Alisha Pramod2, Grace Philip3, Deepika E D4, S. J. G. 1Mangalam. (2019). Sybil Attack Detection in Vanet Using Spider-Monkey Technique and Ecc. International Journal of Wireless Communications and Network Technologies, 8(3), 31–34.

[22] Al-Mutaz, M., Malott, L., & Chellappan, S. (2014). Detecting Sybil attacks in vehicular networks. Journal of Trust Management, 1(1), 4.

[23] Ayaida, M., Messai, N., Najeh, S., & Boris Ndjore, K. (2019). A Macroscopic Traffic Model-based Approach for Sybil Attack Detection in VANETs. Ad Hoc Networks.

[24] Baza, M., Nabil, M., Bewermeier, N., Fidan, K., Mahmoud, M., & Abdallah, M. (2019). Detecting Sybil Attacks using Proofs of Work and Location in VANETs. ArXiv:1904.05845v1 [Cs.CR] 11 Apr 2019.

[25] Chawla, A., Kumar Patial, R., & Kumar, D. (2016). Comparative Analysis of Sybil Attack Detection Techniques in VANETs. Indian Journal of Science and Technology, 9(47).

[26] Dutt, K. J., & Joshi, S. B. (2019). Defending Against Sybil Attacks by Enhanced Event Based Reputation System in Vanet. International Journal of Engineering and Advanced Technology, 9(2), 4445–4450.

[27] Feng, X., Li, C. yan, Chen, D. xin, & Tang, J. (2017). A method for defending against multi-source Sybil attacks in VANET. Peer-to-Peer Networking and Applications, 10(2), 305–314.

[28] Girija, M. K., & Saravanan, K. S. (2017). Attack Resistant VANET Data Communication using Vehicle Movement Behavior Analysis. International Journal of Modern Trends in Engineering & Research, 4(9), 100–106.

[29] Golle, P., Greene, D., & Staddon, J. (2004). Detecting and correcting malicious data in VANETs. VANET - Proceedings of the First ACM International Workshop on Vehicular Ad Hoc Networks, 29–37.

[30] Gu, P., Khatoun, R., Begriche, Y., & Serhrouchni, A. (2017). K-Nearest Neighbours classification based Sybil attack detection in Vehicular networks. Proceedings of the 2017 3rd Conference on Mobile and Secure Services,

MOBISECSERV 2017, 1–6.

[31] Hamdan, S., Hudaib, A., & Awajan, A. (2019). Detecting Sybil attacks in vehicular ad hoc networks. International Journal of Parallel, Emergent and Distributed Systems, 1744–5779.

[32] Hamdan, S., Hudaib, A., & Awajan, A. (2019). Hybrid Algorithm to Detect the Sybil Attacks in VANET. 5th International Symposium on Innovation in Information and Communication Technology, ISIICT 2018.

[33] Iwendi, C., Uddin, M., Ansere, J. A., Nkurunziza, P., Anajemba, J. H., & Bashir, A. K. (2018). On Detection of Sybil Attack in Large-Scale VANETs Using Spider-Monkey

[34] Kaur, K., & Kaur, A. (2018). Detection of Sybil Attack in VANETs. International Journal of Emerging Research in Management and Technology, 6(6), 296.

[35] Khalil, M., & Azer, M. A. (2018). Sybil Attack Prevention through Identity Symmetric Scheme in Vehicular Ad-Hoc Networks. 2018 Wireless Days (WD), 184–186.

[36] Mishra, D. P., & Asutkar, G. M. (2016). A Novel Approach to Detect Sybil Attack in VANET. International Journal of Innovative Research in Science, Engineering, and Technology, 5(10), 17802–17820.

[37] Mohassel, P., & Zhang, Y. (2017). SecureML: A System for Scalable Privacy-Preserving Machine Learning. Proceedings - IEEE Symposium on Security and Privacy.

[38] Panchal, A., & Singh, D. D. (2017). Segregation of Sybil Attack using Neighbouring Information in VANET. Iarjset, 4(6), 172–180.

[39] Pattanayak, B. K., Pattnaik, O., & Pani, S. (2020). A novel approach to detection of and protection from Sybil attack in Vanet. Lecture Notes in Networks and Systems, 109, 240–247.

[40] Pavan Kumar, B. V. S. P., & Sharma, S. S. V. N. (2019). Hash-based co-operative method to handle Sybil attack sequences in vehicular ad hoc networks. International Journal of Engineering and Advanced Technology, 8(6 Special issues), 993–999.

[41] Sujatha, V., & Mary Anita, E. A. (2019). Identity-based scheme against Sybil attacks in wireless sensor networks. International Journal of Engineering and Advanced Technology, 9(1), 5350–5355.

[42] Velayudhan, N. C., Anitha, A., Madanan, M., & Paul, V. (2019). Review on avoiding Sybil attack in VANET while operating in an urban environment. Journal of Theoretical and Applied Information Technology, 97(20), 2267–2279.

[43] Maleknasab Ardakani, M., Tabarzad, M.A. & Shayegan, M.A. Detecting Sybil attacks in vehicular ad hoc networks using fuzzy logic and arithmetic optimization algorithm. J Supercomput 78, 16303–16335 (2022). https://doi.org/10.1007/s11227-022-04526-z

[44] Lim, K., Tuladhar, K. M., & Kim, H. (2019). Detecting Location Spoofing using ADAS sensors in VANETs. 2019 16th IEEE Annual Consumer Communications and Networking Conference, CCNC 2019, 9–12 https://doi.org/10.1109/CCNC.2019.8651763