Detecting Sybil Attack in Vehicular Ad-hoc Networks (Vanets) by Using Fitness Function, Signal Strength Index and Throughput

Article *in* Wireless Personal Communications · April 2022

DOI: 10.1007/s11277-021-09261-x

CITATIONS
24

READS
449

2 authors:

Seyed Salar Sefati
Polytechnic University of Bucharest
28 PUBLICATIONS **383** CITATIONS

SEE PROFILE

Sara Ghiasi
3 PUBLICATIONS **44** CITATIONS

SEE PROFILE

Wireless Personal Communications
https://doi.org/10.1007/s11277-021-09261-x

Detecting Sybil Attack in Vehicular Ad-hoc Networks (Vanets) by Using Fitness Function, Signal Strength Index and Throughput

Seyed Salar Sefati[1] · **Sara Ghiasi Tabrizi**[2]

Accepted: 19 October 2021

Abstract
Ad-hoc networks are vehicular networks whose functions are widely expanding. High dynamicity and the presence of wireless communications are two major challenging features of these networks. Due to, security and protection of these networks have remained as big unresolved challenges. Attack detection in Vanets may have significant impact on the efficiency of these networks. Timely detection of attacks helps prevent road casualties and traffic control. Initial identification is done by the neighboring nodes. When each node receives a message from neighboring nodes, it compares the ID of each node's with those of other nodes' messages. If the messages are the same but sent from different nodes, neighboring nodes send a sample of the data to the RSU. If RSU doubts to an ID, it establishes a table of parameters, such a delay, packet drop and throughput. The total sum of fitness function should be equal to one. If the fitness function of these parameters is beyond the determined limit, nodes will continue to work. In this paper detected Sybil attacks used by the NS3 simulator. The results of the proposed method were acceptable in comparison with PDF (probability density function), FCVS (Fuzzy-based collaborative verification system) and Heartbeat scheme. Delay, energy and strength were the parameters, which had higher responsiveness.

Keywords Vehicular Ad-hoc networks · Mobile Ad-hoc networks · Sybil attacks · Signal strength index

1 Introduction

In the last decade, due to the rapid development and expansion of technology and communication and diverse humans' needs, the necessity and requirement of wireless networks is felt more than before [1]. Vehicular ad hoc networks (Vanets) are regarded as a subset of

✉ Seyed Salar Sefati
Seyedsalarsefati@gmail.com

[1] Faculty of Electronics, Telecommunications and Information Technology, POLITEHNICA University of Bucharest, Bucharest, Romania

[2] Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran

Mobile Ad-hoc Networks (Manets). There is a set of nodes among vehicles which establish wireless communications with each other. Fast movements of vehicles and the shortness of connection time are regarded as the features of these networks [2]. The rationale behind Vanets is to establish security and convenience for drivers and passengers [3]. In this regard, many efforts have been made to prevent car accidents and improve traffic status. In Vanets, each vehicle is equipped with a technology which allows drivers to communicate with each other and with road infrastructure. Infrastructures of roads, known as Road Side Units (RSU) are located at some critical points such as near traffic lights or near Stop signs on roads and streets [4]. They are aimed at improving traffic status and making driving more secure [5]. In Vanets, vehicles, moving in urban and suburban areas, can potentially diffuse and share their vehicles' data and the data received from the surrounding environment to other vehicles [6]. In addition, they can use the data received via RSU equipment. A great percentage of accidents is attributed to the lack of drivers' awareness of obstacles and problems on the roads ahead of them. Nevertheless, Intelligent Traffic System (ITS) can provide conditions which may significantly contribute to enhancing drivers 'awareness of the dangers and probable obstacles on the way forward [7]. Each vehicle can obtain information regarding safety issues such as messages for avoiding accident, traffic, collision situation and other information like weather condition and tourism information [8].

Security issues in Vanets are of critical significance. Different methods have been proposed for detecting attacks among vehicles. One of the present attacks in these networks is known as sybil attack; it severely disrupts network performance and endangers network security by disrupting many protocols [9]. Sybil attack may work on three dimensions: direct vs. indirect, fabricated identity attack vs. stolen identity and simultaneous attack vs. non-simultaneous attack. Regarding direct communication, the invader directly establishes communications with real nodes and draws traffic towards it [10].In indirect communications, the invader does not communicate directly with the real nodes; rather, it establishes communications with the real nodes through one or many Sybil nodes. Many research studies have been conducted on the strategies for dealing with these attacks; nevertheless, these attacks cannot distribute accurate information about themselves due to the forgery of identity information [11]. It should be noted that these networks have specific application range and limit; that is, they are generally applied in highly critical and confidential environments [12]. Consequently, data accuracy and security in these networks is of high significance. Wireless sensor networks (WSNs) are inherently vulnerable to attacks [13]. Restrictions such as limited resources, unreliable communications, unattended automatic operations, etc., may make it impossible to apply security techniques of traditional networks in these networks [14]. Communication channel, used by sensor nodes for communicating and exchanging information [15], is regarded as one of the important issues and challenges in these networks. Indeed, the communication channel in this regard is air which may be inevitably used and shared by others, namely invaders [16]. Hence, since our communication channel is the same as that used by invaders, specific techniques should be used for preserving and maintaining data accuracy, on the one hand; on the other hand, the network should keep operating [17]. This condition enhances and highlights the significance of security in this type of network in comparison with other networks. Security should be established in such a way that it is compatible with the available limitations of these networks. Also, it should satisfy the requirements of these networks [18].

In this paper, Initial identification is done by the neighboring nodes. When each node receives a message from neighboring nodes, it compares the ID of each node's with those of other nodes' messages. If the messages are the same but sent from different nodes, neighboring nodes send a sample of the data to the RSU. If RSU doubts to an ID, it establishes

a table of parameters, such a delay, packet drop and throughput. The total sum of fitness function should be equal to one. If the fitness function of these parameters is beyond the determined limit, nodes will continue to work. Nonetheless, in case the determined limit is below the defined limit, we will again compare the suspicious nodes by using the received signal and their throughputs. In case the node's throughput is less than the mean throughput of all the nodes, it will be regarded as a malicious node; hence, it will be thrown away from the network. The contributions of the present study are as follows:

- Detecting the malicious nodes by having each node's data by means of fitness function
- Receiving initial data related to the behavior of each node by using that node's neighbors so as to prevent misleading and deception of the malicious node
- Establishment of a table of parameters which is compatible with network structure for gathering accurate data for reducing detection time

The rest of the paper is organized as follows: Section 2 reports related works. Section 3 introduces and explains the propose method. Section 4 discuses experimental dataset used in the study and simulation results. Section 5 presents a discussion of the results, draws the conclusion of the paper and gives directions for further research.

2 Related Works

Verma et al. [19] proposed an efficient method which can identify all malicious IP addresses. By relying on filtering, they put forth a data structure which is storage-dominant; it only needed a fixed-length table for recording data on vehicle traffic. Then, this method was executed for detecting sudden changes regarding traffic features of vehicles in relation to the occurrence of Sybil attacks. The adopted method uses Bloom filter for the filtering process. It is appropriate for smaller scale Denial-of-service attack (DOS) attacks as well as larger scale ones. Simulation results indicated that detection rate is enhances when the desired number of nodes is forged by invaders.

Iwendi et al. [20], focused on large-scale Vanets. They proposed Spider Monkey Time Synchronization (SMTS) which has been biologically simulated. The proposed method was designed according to meta-heuristic stimulation via spider monkey operations. A SMTS method was used for investigating techniques in Vanets. In this way, it was aimed at resolving the expectation of different collisions with vehicles in challenging areas. Furthermore, a pseudo-code algorithm is proposed which is continuously diffused in one-way package delivery scenarios. As a result, release delay and off-time adjustment in the transmission of packet traffic lights message are properly diffused to the vehicles. Given the extent of intrusion detection, measurement precision and energy efficiency were carried out properly in longer transmission distances for detecting Sybil attacks in Vanets.

Yu et al. [21] proposed a collaboration technique for assessing the physical position of the suspected node. There are two available methods for solving the challenges, i.e. statistical detection and evidence system. The attacks initiated by drivers can be effectively suppressed by these methods. The real-life simulation of USA maps along with the traffic models proves the performance and efficiency of this scheme. Indeed, it was proved that an economic approach was used for suppressing SA without any further support from the positioning hardware. The shortcoming of this method is that this method initiates only

fundamental infrastructure notions such as presence evidence system and channel noise estimation. Another drawback of this method is that reading signal strength is not precise.

Sarigiannidis et al. [13],proposed an anomaly detection strategy which is called Rule-centric Anomaly Detection Strategy (RADS) which, used in huge WSNs. Accordingly, axis range detection algorithm, with a wide bandwidth, operates in such a way that there is no need for sharing resources or collaboration among sensor nodes for detecting anomalies. The probability of the recommended strategy was analytically confirmed. The performance of RADS was widely evaluated with regard to exposing attacks in terms of numerical and mathematical aspects. Hence, anomaly detection can be statistically diagnosed. The obtained results indicated that RADS has achieved higher detection precision and lower false alarm rate.

Chen et al. [22], recommended secured ambulance communication protocol which is targeted at Vanets. It ensures that messages are not exposed to contamination or they are not eavesdropped. The proposed system includes symmetric encryption, digital signatures and MAC approaches. In this way, it has achieved non-denial, availability, known key security, integrity, confidentiality, session key security, cross-authentication, and the ability to escape from known attacks. Finally, actual vehicle congestion statistics was obtained by NS3 results on Taipei city road map.

Fogue et al. [23] , proposed a common and active strategy for confirming the position of neighbors based on the information which is exchanged between neighbors. They called it CNPV protocol which easily adapts to different modes of broadcasting warning messages. It makes use of neighbor's details for selecting the related transportation strategy in Vanets. By diffusing a message, CNPV limits the confirmation permission of neighbors' positions before the next transportation vehicle is selected. Next, the performance of CNPV protocol is evaluated by pairing it with diffusion algorithm. They can demonstrate how the presence of enemy nodes impacts on the performance with regard to urban cases. CNPV can help mitigate aggressive effects.

Jamshidi et al. [24], presented a model in cluster-oriented WSNs which is called Leach. Then, an algorithm based on Received Signal Strength Indication Distance (RSSI) and the combination of cluster-head nodes was proposed for protection against the initial sample of attack. Furthermore, its performance was evaluated in relation to total delivery rate and system overhead. Experimental results indicated that profitable algorithm imposes little relation to the network and it can observe 99.8% of Sybil nodes with average 0.08% FDR.

3 Vehicular Ad-Hoc Networks

Vanets are multiple networks without fixed infrastructures. These networks include vehicles in motion which can communicate with each other [25]. In fact, Vanets are wireless mobile networks which provide the ability for establishing communication among vehicles; they are aimed at providing and maintaining road security and safety via exchanging warning messages among adjacent vehicles; also they provide new services for road users. The rationale behind inter-vehicular systems is to establish and maintain safety and security for drivers and passengers. In this regard, a lot of efforts have been done so as to prevent accidents and optimize traffic status. In Vanets, each vehicle is equipped with a technology which allows drivers to communicate with each other and with road infrastructures. They are located at some critical spots of streets and roads like traffic lights at intersections or at

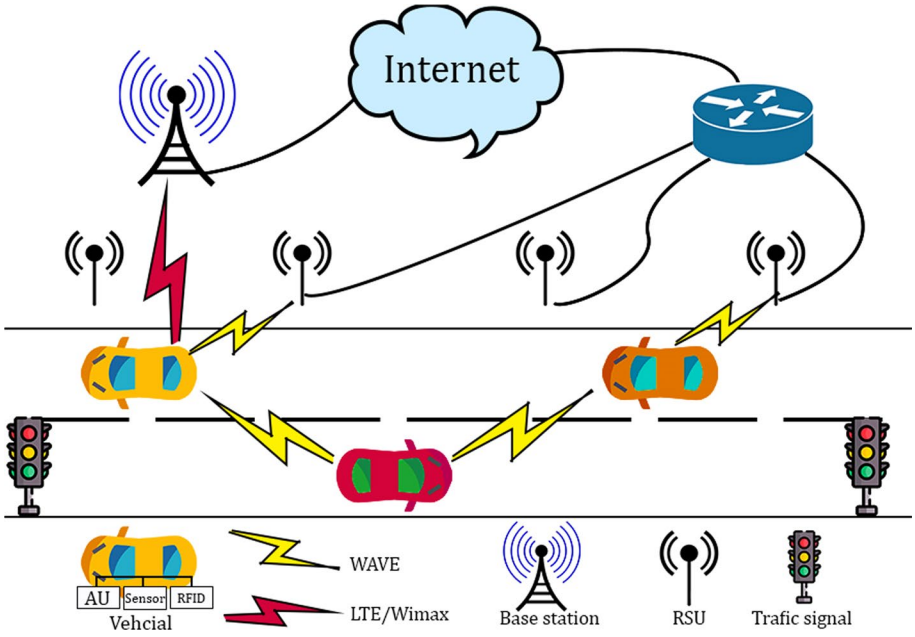

Fig. 1 Architecture of Vanet system

stop signs. In this way, they are designed to help improve traffic status and make driving safer and more secure for drivers and passengers. Figure 1 shows the Vanets architecture.

3.1 Communication Pattern Among Nodes

Vanets provide the opportunity for establishing communication among vehicles and sending data about road conditions and other required data among vehicles [26]. Inter-vehicular communications are aimed at exchanging data and messages in two ways: Vehicle-vehicle communications (V2V) and Vehicle to Infrastructure Communications (V2I). In V2V, data is exchanged among vehicles only via Intermediate vehicles and with a multi-step communication approach. In this communication pattern, each vehicle plays the roles of both host and a router in the network. On the other hand, in communications via RSUs, a base station, at the road side, plays the interface role among vehicles for exchanging data. Figure 2 depicts communication pattern among vehicles. As shown in this figure, the occurrence of events is reported to the base station at the road side via several intermediate vehicles. Also, it allows for inter-vehicular communication without using infrastructure equipment. It allows data diffusion to be used in application programs with regard to safety and security. In this case, RSUs and other wireless communication equipment such as access points are connected to each other by means of WiMax30 cellular workstations which are probably wired. They provide the opportunity for establishing wireless communications with vehicles (the final communication step) so as to have access to internet, gather traffic information and other routing purposes [27]

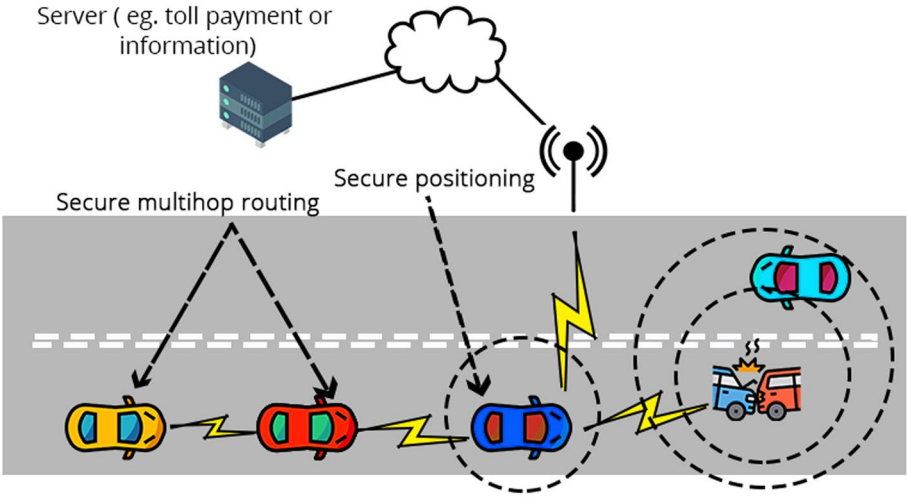

Fig. 2 Model of data transmission and communication within vanet

3.2 Nodes' Data Transmission Radius

An increase in traffic and vehicle congestion throughout a route leads to reduced distance among vehicles on the road. This issue is attributed to reduced speed of vehicles' movements and heavy traffic throughout the route. Hence, occurrence of an accident throughout the route such as car collision is regarded as the most significant reason for the reduction in vehicles' movements throughout the route. Simultaneous speed reduction throughout the route leads to reduced distance between nodes in the network. As a result, more nodes are placed within each other's sending radius. Thus, it can be maintained that the speed of nodes' movements is inversely related to the extent of their overlap within the network. In this way, as the speed of nodes' movements increases, the degree of their overlap decreases. The simultaneous reduction in nodes' movement speed, in Vanets, results in increased network density along the route. Vehicles are allowed to establish communications with each other without using infrastructure equipment; also, application programs are used for achieving safety, security and information diffusion. This area is related to intra-vehicular communications as network nodes which include a communication and processing equipment, referred to as On-Board Unit (OBU); it is capable of establishing wireless communications by using DSRC technology so that they are connected to other machines. This area has one or more Application Units (AU); each AU is an applied machine or it executes one or more applications by capitalizing on OBU communication capability. The communication between AU and OBU may be wired or wireless including the following technologies: WUSB34 (Wireless USB), Bluetooth and UWB (Ultra wideband). By being connected to OBU, it can be constantly installed on the vehicle. Figure 3 show's the data transmission manner.

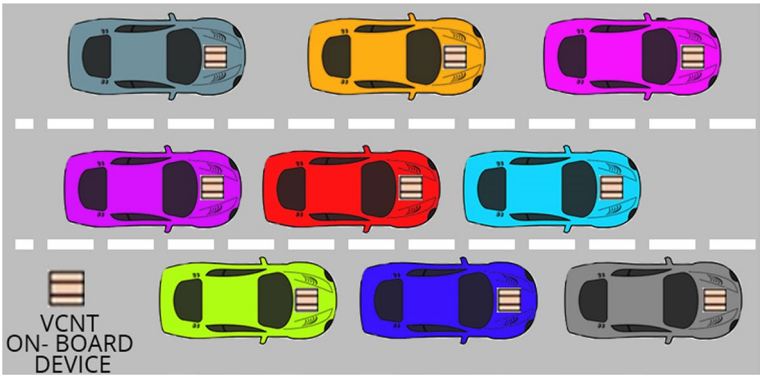

Fig. 3 Data transmission manner

3.3 Security in Vehicular Networks

Since lots of information is distributed and broadcast in Vanets, security is of high significance. Vehicles can easily and securely send or receive location-based messages without being worried about surveillance cameras. In general, if security measures are not taken in vehicular networks, malicious nodes can obtain nodes' source and destination information; that is, by using the databases of positioning maps such as Google map or Baidu map, they can easily obtain the home and work addresses of a vehicle node. Hence, security mechanisms should be predicted for dealing with security attacks in vehicular networks. An element that is the environment of Event data recorder (EDR) hardware modules, which are available in various types including Tamper Proof Device (TPM) and Trusted Platform Module (TPD) security, which are the most common. TPM is a reliable platform module; it is a hardware module which can be installed on vehicle. It has been designed for security objectives such as secure computations and reliable data storage. It can be integrated with any other device such as laptop or personal computer. This hardware piece needs a software infrastructure for establishing communication so that it can store and protect data in a safe and reliable location. It can be resistant to software attacks but it is not resistant to hardware damage. Secure Hash Algorithm Version 1.0 (SHA), RSA and Random Number Generators (RNG) are key cores of this module which conduct data encryption operations. In general, three key capabilities of this module are: data protection, data accuracy measurement and reporting data accuracy.

3.4 Sybil Attack & Threshold

Vehicular networks operate in wireless environments. Hence, they are vulnerable to security attacks. Due to network structure, the required security construction of these networks is highly complicated. Given different attacks which threaten these networks, in this paper, we focused specifically on Sybil attack which is regarded as the root of many attacks and threats in this network. Sybil attack was firstly taken into consideration by Douceur in peer-to-peer networks. These attacks are regarded as a threat for network security. A malicious Sybil node generates fake IDs; or by forging nodes' ID within the network, it introduces itself as a normal node. By eavesdropping the transmitted messages within the network,

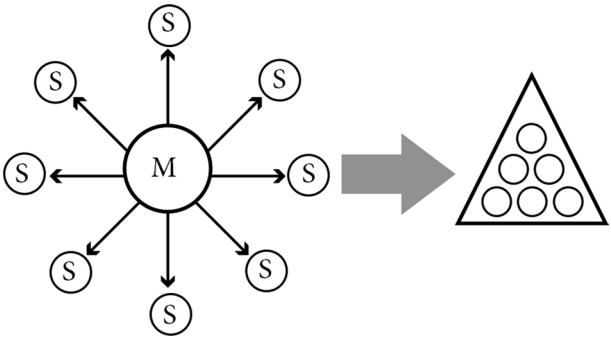

Fig. 4 A scheme of a malicious node and Sybil nodes generated by this node

malicious nodes steal and forge the ID of the nodes which send messages. Since vehicles are always in motion in Vanets, network density and topology change frequently. For updating their routing table with regard to other vehicles, vehicles should continuously communicate with each other. Malicious nodes exploit this feature of the network and carry out their Sybil attack on network vehicles. Consequently, several nodes with fake IDs are produced in the network. A malicious node produces several nodes as Sybil nodes and it forges IDs for all these fake nodes. Figure 4 depicts a scheme of a malicious node and the generated Sybil nodes. The purpose of a malicious node is to deceive normal nodes of the network. In this way, they are made to think that they have many neighbors but, in fact, those nodes do not exist. Several network protocols such as voting protocols, data aggregation, etc., are severely disrupted and disabled.

Traffic pattern changes in a network in which there are some malicious nodes that start Sybil attacks. By creating multiple Sybil nodes and having multiple IDs, malicious nodes play the roles of several nodes in network routing. This situation leads to increased proximity and closeness of nodes. Figure 5 gives a depiction of a network with some nodes and

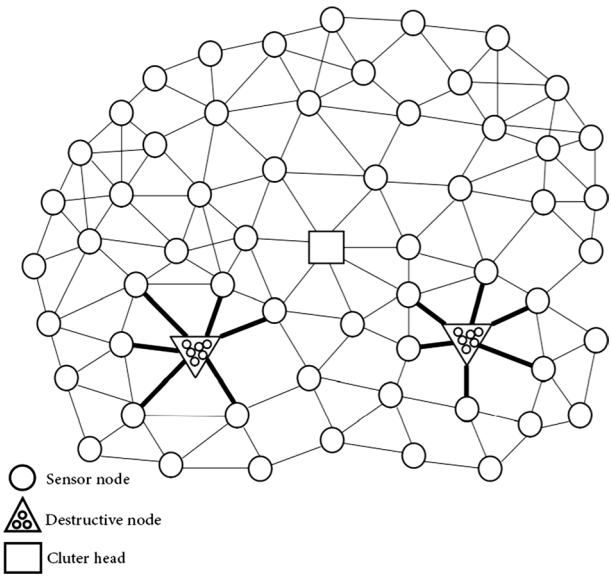

Fig. 5 A network with two malicious nodes

two malicious nodes. As shown in figure, malicious node performs the roles of several nodes and sends data packets.

In the proposed method, threshold is determined based on the location of the base station, history of the number of vehicles passing through the route and road width. Base station is considered in two locations: inside and outside the urban range. Regarding the urban limit, threshold value is equal to one. As a result, nodes' sending radius, in urban areas, is equal to their movement speed. However, it should be noted that vehicles' complete stop in urban areas is usually due to heavy vehicle traffic. In this regard, when vehicles' speed is zero, the distance between vehicles reaches the shortest possible amount. Hence, given the installation location of the transmitting machine in vehicles, when vehicles' speed in urban areas is zero, their transmission radius will be equal to twice the length of the car. In this equation vehicle length is denoted by unit of meter. Hence, with respect to the installation location of the transmitting machine in vehicles, when vehicles' speed is zero in urban areas, their transmission radius will be twice the length of the machine. The following equation measures node's transmission radius. Nodes' transmission radius in urban areas is measured by Eq. 1. In this equation CL denotes vehicle length with Meter unit.

$$T_r = \begin{cases} VV > 0 \\ 2 * CLV = 0 \end{cases} \tag{1}$$

In areas outside of the urban range, nodes' speed is variable and vehicles' dispersion is high. Moreover, in these areas, vehicles move at high speed along the route. However, it should be noted that threshold parameter T is measured by the base station and is sent to the vehicles. Moreover, another parameter which has impact on threshold determination is road width. Hence, vehicles which pass through a wider road are distinguished from those vehicles which pass through a narrow road. According to the above-mentioned discussion, threshold parameter for determining nodes' transmission radius in suburban areas is measured via Eq. 2.

$$t = \frac{V_C}{\frac{B_M}{L}} \tag{2}$$

In this equation, V_c refers to average speed of nodes' movement along the route in kilometers per hour. L denotes road width in terms of the number of lanes for vehicles movements. $\frac{B_M}{L}$ refers to the history of the number of vehicles on the route. In Eq. 2, the width of roads L is always a constant value. Given road conditions, L parameter is at the disposal of base stations at road sides for measuring threshold parameter. On the other hand, in this equation, average V_c and the number of vehicles on the road are variable. In this regard, speed, the number of speeds of vehicles' movements and the length of the route can be predicted by using the history of moving vehicles. On the other hand, as the traffic on the route length decreases and route density decreases simultaneously, average speed of vehicles can be measured at longer time intervals. In other words, as route vehicle decreases, standard deviation of vehicles' movement speed decreases. Hence, vehicles move fast close to each other. According to the above-mentioned discussion, regular time intervals T_i are measured via Eq. 3 to zero the average speed of nodes.

$$T_i = \frac{1}{B_m} \tag{3}$$

Hence, the proposed method in each $\frac{1}{B_m}$ hour, average speed of vehicles' movement is reset to zero. Given the above-mentioned parameter, it was observed that the number of vehicles along B_m is inversely related to regular time intervals of zeroing vehicles' movement speed T_i. At regular time intervals T_i, the proposed method sets the average number of vehicles to zero and re-measures them. It should be noted that the history of vehicles' movements along a route is different at different times.

3.5 The Proposed Method

- The receiving node requests message and the neighbour sends it

When a new node is added to the vanet, it needs to receive information from other nodes which start to receive information.

- The nodes sending the rates have different IDs. In case message information is identical, the head-cluster is informed of it. Otherwise, the operation continues.

In Sybil attack, it is possible to send inaccurate information via the neighbouring node. For example, in Fig. 6, the malicious node C_j sends different IDs from itself (C_h, C_k) at different positions. Two Sybil nodes C_k and C_h send information about their position. (idh; xh; yh), (idk; xk; yk) are sent with two different IDs (id_h and id_k) to the node M by Sybil node C_j. If the sent position by the node is considered to be RSS, the malicious node can be tracked with regard to Eq. 1. In this way, RSS_{ji} and RSS_{ki} are two different positions of the nodes k and J from node i.

$$S = \begin{cases} 1, if \left| RSS_{ji} - RSS_{ki} \right| \leq t \\ 0, otherwise. \end{cases} \tag{4}$$

- Notifying RSU:

In case the receiving nodes are in doubt, they inform RSU.

- Nodes' locations are identified by RSU and it orders them to read information

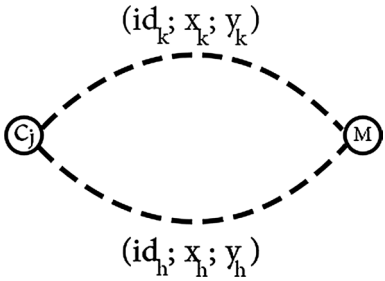

Fig. 6 An example of Sybil attack

When it doubts a node, the order for identifying and detecting the location of the node is given by the sink.

- After doubting nodes with Sybil attacks, a table of parameters is generated.

The performance of each group of protocol parameters regarding vanet is evaluated by means of three parameters of Quality of Service (QoS):

PDR: (average packet delivery rate): it refers to the ratio of successfully delivered data packets to the destination to the total number of packets sent from the source. This parameter indicates how successful was the protocol in fulfilling its duty, i.e. proper data transmission.

E2ED: (average end-to-end delay): it refers to the total time taken for successfully sending/receiving each data packet.

Power consumption: it denotes the consumption of energy in Vanets due to data packet transmission, packet reception and packet processing. It should be noted that power consumption for packet processing is much less than that for receiving/sending data packets. Vanet sensors on a vehicle are connected to the electric system of the vehicle; consequently, in case sensors consume a lot of energy, it may cause some problems for the vehicle. Power consumption is regarded as one of the fundamental issues in research on Vanets.

Packet loss: in computer networks, packet loss is regarded as a type of service-denial attack; in this attack, the routing, which is aimed at sending packets, throws away some packets; this usually occurs on the side of the routing; it is at risk for various reasons. One reason mentioned in the research studies is attributed to service-denial attack in the router. Since packets are usually removed in high-cost networks, predicting and detecting packet removal attack are very challenging.

- Nodes' threshold is determined by using road and vehicle conditions. Then, using fitness function, the specified limits of parameters are measured.

Each node's threshold function is firstly measured with regard to urban or non-urban conditions. Next, fitness function, which is used optimization issues, is measured. In optimization problems, the objective is to minimize or maximize fitness function which is defined depending on the problem type. In line with optimizing QoS, the main objective is to maximize PDR, minimize power consumption, E2ED and packet loss. Equation 4 gives fitness function which has been defined for this study. As shown in this equation, a minimization formula was used for fitness function. Accordingly, PDR is placed in the formula with a negative sign. Factors W_1, W_2, W_3, W_4 are equal to the weights which determine the impact of each evaluation parameter on function results. Here, the values of W_1, W_2, W_3, W_4 are 0.2, 0.2, 0.2, 0.4, respectively.

$$Fitness = w_1 * (-pdr) + w_2 + * NRL + w_3 * E2E + w_4 PD \tag{5}$$

If($L_{vm\,j} \leq \psi$)

Nodes is under loaded

Else if ($Lvmj \geq \psi$)

Nodes is over loaded

End

The determined limit in each node's fitness function can be measured in the following way:

$$y = AL + s \tag{6}$$

AL denotes average fitness function of doubtful nodes. σ stands for standard deviation of average fitness value regarding doubtful nodes. Average load of doubtful nodes is measured by using the following formula. In this formula, M stands for the number of nodes in a network.

$$AL = \frac{1}{m}\sum_{j=1}^{m} L_{vmj} \tag{7}$$

In this way, standard deviation of fitness function for all the nodes is measured by the following formula:

$$AL = \sqrt{\frac{1}{m}\sum_{j=1}^{m}\left(L_j - AL\right)} \tag{8}$$

σ stands for the SD of fitness function regarding all the nodes. AL refers to the average fitness function of doubtful nodes. L_j stands for the j node's load. M refers to the number of nodes.

Thus, if the value of fitness function on each of the nodes is higher than the determined amount, that node is regarded as a busy node. As a result, it is suspected for Sybil attack. Hence, attacking nodes should be discovered; otherwise, it will be regarded as a normal node.

- Starting of the signal strength index detection algorithm:
- Measuring each node's signal strength and power:

In most cases, after Sybil attack, nodes' signal strength and power have a descending trend. Thus, nodes are gradually demolished or it makes other nodes to make mistakes.

$$R_i = P_0 K / d_i^a \tag{9}$$

P_0 denotes the sender's power; R_I indicates RSSI; K is a fixed number. D_i is Euclidean distance. A is power-distance gradient. RSSI rate is measured by the following formula:

$$R_i / R_j = \left(\frac{P_0 K}{d_i^a}\right) / \left(\frac{P_0 K}{d_j^a}\right) = \left(\frac{d_j}{d_i}\right) \tag{10}$$

- Saving the saved parameters in the search table:
- Measuring signal strength and throughput:

In case the values of a node's throughput and signal strength are below the average of other nodes' values, it will be eliminated from the network; then, a message is sent to other nodes.

Packet ID
Packet Type
Cluster ID

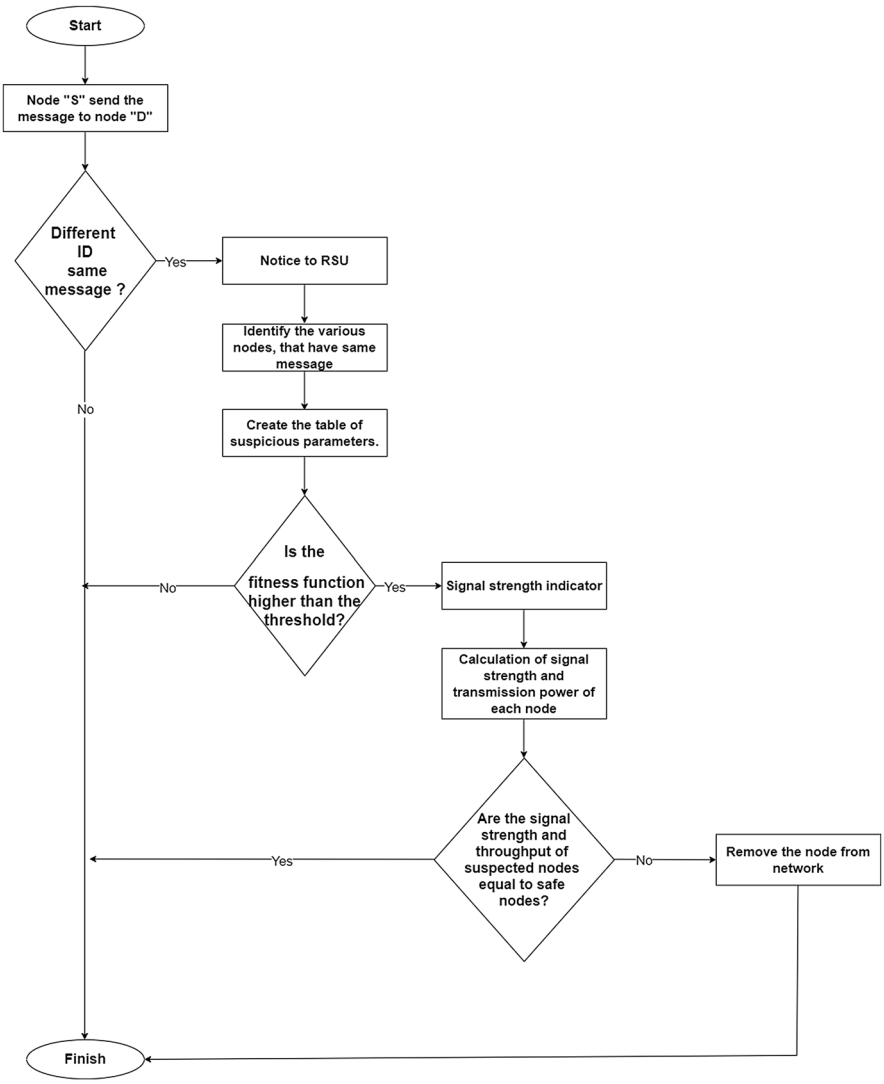

Fig. 7 Flowchart of proposed method

reliable list
suspicious list

Nevertheless, if the values of a node's signal strength and throughput are beyond or equal to other nodes' values, they will be re-examined. Figure 7 depicts the proposed method flowchart.

4 Scenario of Simulating Vehicular Ad-Hoc Networks (Vanets)

We used NS3 network simulator for simulating Vanets in this study. In this scenario, 140 vehicles are moving in an urban area with the dimension 670*670 square meters for 3 min. Throughout the simulation time, a number of vehicles are exchanging messages with each other. Since vehicles' movements is in an urban area, their speed varies from 10 to 50 km/h. The size of transmitted packets among vehicles is 512 bytes; packet transmission rate by each vehicle in this network is $\frac{Packets}{s}$. In this scenario, transmission protocol is of UDP type. Ad hoc On-Demand Distance Vector (AODV) routing protocol was used for routing. Table 1 gives a synopsis of the simulated parameters.

Simulation time was 50 s. Size was 50*50 square meters. A Constant Bit Rate (CBR) was defined as simulated traffic. As shown in Table 1, the applied parameters for measuring performance are as follows: 1. average package delivery ratio, 2. the remaining energy 3. Production capacity, 4. Lost packets.

4.1 Varying Number of Attackers

The performance of the proposed method is analyzed with performance metrics. Based on the Sybil node attack detection and security control of proposed method, the performance of VANET network is developed under attacking condition. To prove the efficiency of the proposed method, it is analyzed with performance metrics such as delay, packet loss, and accuracy. Delay can be defined as the time engaged aimed at a packet to be communicated diagonally the network from one node to another destination node. The packet loss is derived as the disappointment of solitary or additional communicated packets to send the destination node from sender. The failure packet data can be considered as the packet loss. Based on the performance metrics, the verification and analysis of proposed method is done. The delay, packet loss of the proposed method should be in low which only considered as best performance system. The proposed method is satisfying the above conditions related to performance metrics. In this paper, two results were obtained via two different methods. Regarding the first result, an attempt was made in relation to the number of attacks that have occurred in the network which had impact on the parameters. In the second result, in relation to the number of nodes that have been affected. In the first

Table 1 Simulation parameters

Value	Parameters
NS3	Simulator
50 s	Simulation time
140	Number of cars nodes
CBR (constant bit rate)	Traffic source
IEEE 802.11 b	MAC Protocol
Omni antenna	Antenna
0.3	Transmission power
0.3	Receiving power
50×50	Area
AODV	Routing Information Protocol
UDP	Transmission protocol
10–50km/h	Cars speed

method, the number of invaders was considered to be five. It was compared with Pprobability Density Function (PDF) [28], Fuzzy-based collaborative verification system (FCVS) [29] and Heartbeat scheme [30]; in most cases, the proposed method had better results than the other methods. Firstly, delay of the proposed method was compared with those of other methods. The results of the proposed method regarding delay were better than those of other methods. In other methods, problems are solved via meta-heuristic methods or fuzzy method. The final method was lower than that of the proposed method. Network delay is a design and performance characteristic of a telecommunications network. It specifies the latency for a bit of data to travel across the network from one communication endpoint to another. It is typically measured in multiples or fractions of a second. As shown in Fig. 8, the degree of delay can be analysed in the following way. The above-mentioned 3 methods had almost similar results. The results of the proposed method were slightly lower than those of other methods; it is attributed to complicated computations which were aimed at measuring fitness function. Figure 8 depicts delay in the following way.

Sybil attacks are always possible in the absence of any logical centralized authority. As there is no centralized entity in VANETs, detection of Sybil attacks is very difficult. Some constraints such as validating all entities simultaneously by all nodes and strict coordination among entities are necessary for detection of a Sybil attack. Accurate detection of Sybil attacks is very important considering that these attacks can disrupt the entire network and cause problems on the roads and especially with regard to drivers' health. The applied algorithm has better responsiveness than other algorithms. As shown in this figure, since the proposed method used 3 methods for detecting Sybil attacks, it had better responsiveness than other algorithms. In the used algorithm, nodes were firstly compared with each other. Then, threshold was measured. Finally, signal strength was detected and throughput was considered with regard to the total mean. Figure 9 shows the results in the following way:

Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss in a Transmission Control Protocol (TCP) connection is also used to avoid congestion and thus produces an intentionally reduced throughput for the connection. If the number of invaders is large and varied, the number of dropped packets increases. For solving this problem, the attacked nodes

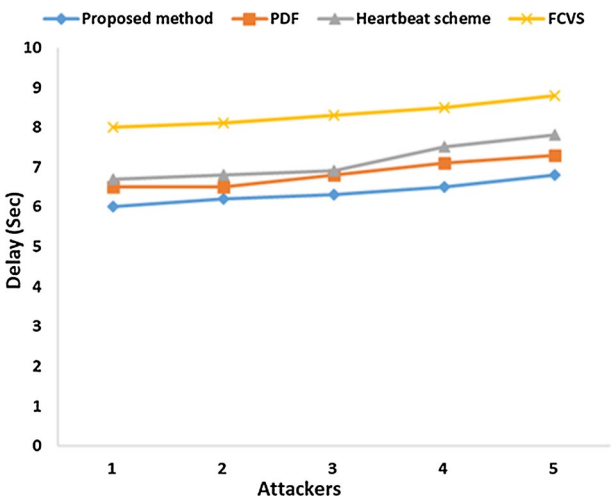

Fig. 8 Invaders vs. delay

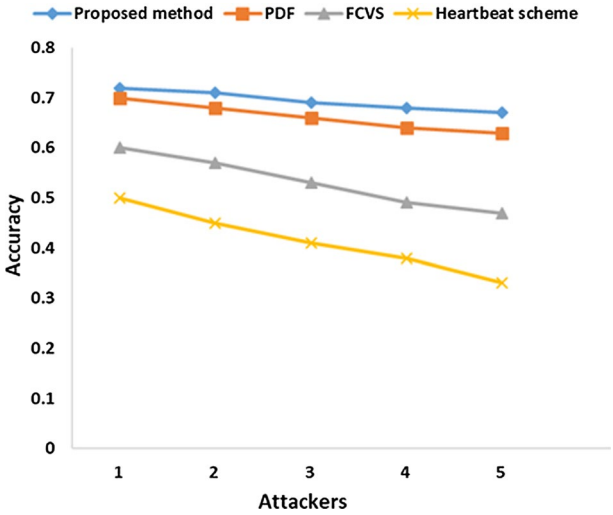

Fig. 9 Detection accuracy vs. attacks

should be quickly discovered; then, RSU should be notified so that it eliminates it from the network. Otherwise, it will encounter the problem of dropped packets. Hence, it can cause many problems in the network. As shown in Fig. 10, dropped packets in the proposed method were fewer than those of other methods. PDF and FCVS methods have obtained closer responses to each other. However, the proposed method could not obtain acceptable response with respect to Heartbeat scheme.

4.2 Based on Nodes

Some experiments were conducted on 60, 80, 100, 120, 140 nodes. As shown in Fig. 11, a change in the number of nodes has an impact on delay parameter. As the number of nodes

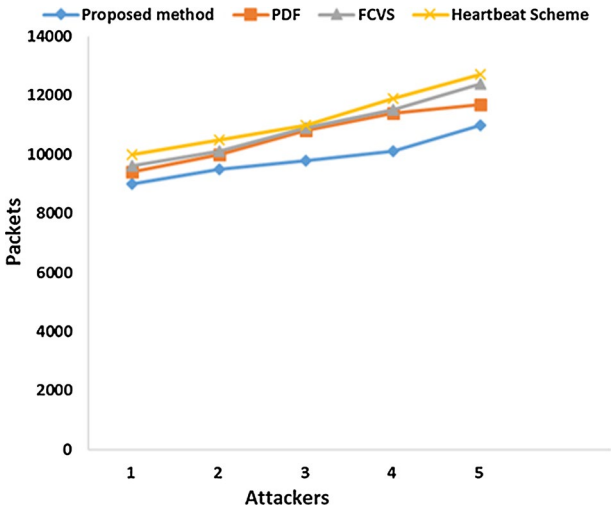

Fig. 10 Dropped packets vs. attacks

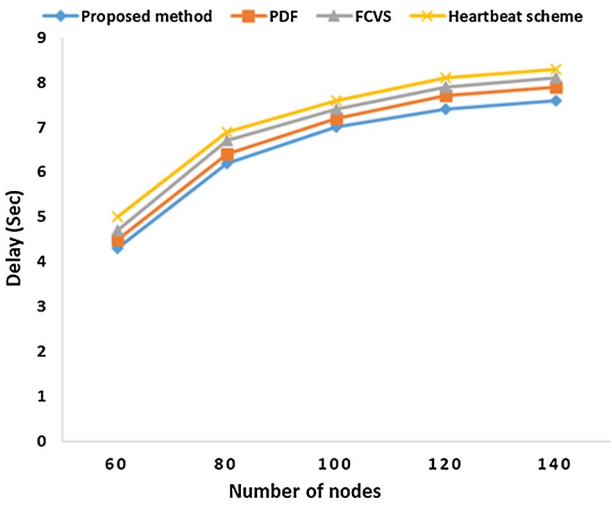

Fig. 11 Nodes vs. delay

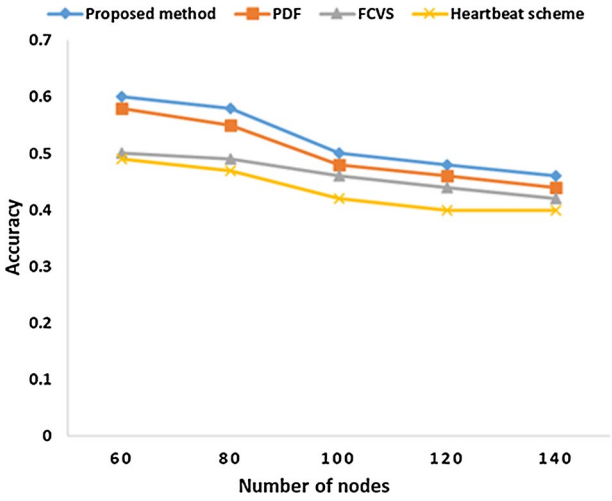

Fig. 12 Nodes vs. detection accuracy

increases, delay in the network increases. Regarding delay parameter, the proposed method achieved the best results in comparison with the other algorithms. Thus, it can be argued that the proposed method managed to minimize delay by using mathematical transactions.

In addition, detection of nodes for attacks are also shown in Fig. 12. As the number of nodes gradually increases the ability to detect those decreases. In this regard, the proposed method had better results than the other methods. Given 140 nodes and 0.5 detection accuracy, the proposed method could perform better than the other algorithms.

Moreover, Fig. 13 depicts the ratio of lost packets to the number of nodes in vanet. As the number of nodes increases, the number of lost packets increases. The proposed method could detect attacked nodes faster and more accurately than the other methods. The proposed algorithm achieved better results than the other algorithms.

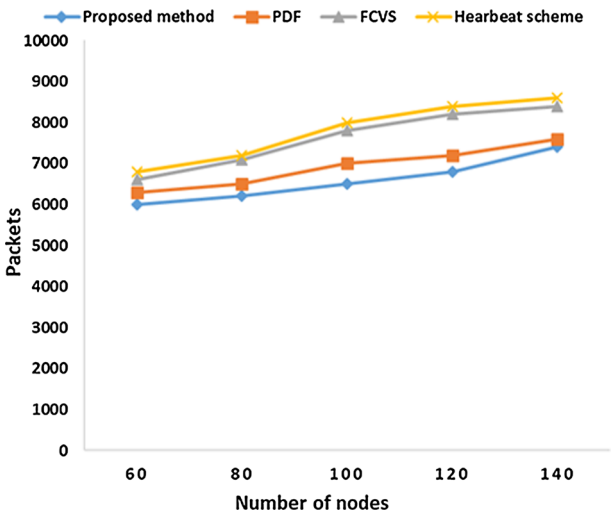

Fig. 13 Nodes vs. lost packets

5 Conclusion and Directions for Further Research

The method proposed in this paper was aimed at preventing network. For optimizing the efficiency of the proposed method, it was supposed to handle congestion and prevent attacks in Vanets. The method proposed in this paper may be used for achieving other objectives such as discovering different attacks and handling intrusion in Vanets. In this paper, by capitalizing on fitness function, signal strength index and throughput, we tried to identify and detect malicious nodes; in this way, we detected Sybil attacks of these networks in NS3 simulator. The results of the proposed method were acceptable in comparison with PDF (probability density function), FCVS (Fuzzy-based collaborative verification system) and Heartbeat scheme. As a direction for further research, future studies can focus on other parameters such as history of fitness function, signal transmission history, throughput history. Accordingly, by considering these parameters, future studies can help reduce attack in the network. Moreover, other methods can be presented for handling network limitations, preventing attacks and optimizing network efficiency. In addition, by imposing some limitations on the movement route of the sent packets within the network, future studies can prevent Sybil attack; as a result, delay in vehicular networks may be controlled. Hence, given the movement limitations of vehicles in Vanets, focusing on the above-mentioned issues may lead to more effective results with regard to preventing Sybil attack.. To sum it up, this line of research can potentially enhance network performance.

Acknowledgment This study has been conducted under the project 'Mobility and Training foR beyond 5G ecosystems (MOTOR5G)'. The project has received funding from the European Union's Horizon 2020 programme under the Marie SkłodowskaCurie Actions (MSCA) Innovative Training Network (ITN) having grant agreement No. 861219.

Declarations

Conflicts of interest The authors confirm that there is no conflict of interest in this research paper.

References

1. Alheeti, K. M.A., Gruebler, A., McDonald-Maier, K. D. (2015). An intrusion detection system against malicious attacks on the communication network of driverless cars. In *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, IEEE, pp. 916–921.
2. Alheeti, K. M. A. Gruebler, A., McDonald-Maier, K. D., Fernando, A. Prediction of DoS attacks in external communication for self-driving vehicles using a fuzzy petri net model. In *2016 IEEE International Conference on Consumer Electronics (ICCE)*, IEEE, pp. 502–503.
3. Bian, C., Zhao, T., Li, X., & Yan, W. (2015). Boosting named data networking for data dissemination in urban VANET scenarios. *Vehicular Communications, 2*(4), 195–207.
4. Faisal, S. M., & Zaidi, T. (2020). Timestamp Based Detection of Sybil Attack in VANET. *Int. J. Netw. Secur., 22*(3), 397–408.
5. Cheng, J., Cheng, J., Zhou, M., Liu, F., Gao, S., & Liu, C. (2015). Routing in internet of vehicles: A review. *IEEE Transactions on Intelligent Transportation Systems, 16*(5), 2339–2352.
6. Yao, Y., et al. (2017). Voiceprint: A novel Sybil attack detection method based on RSSI for VANETs. In *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN),*: IEEE, pp. 591–602.
7. Sefati, S., Mousavinasab, M., Zare hFarkhady, R. (2021). Load balancing in cloud computing environment using the Grey wolf optimization algorithm based on the reliability: performance evaluation. *The Journal of Supercomputing*, https://doi.org/10.1007/s11227-021-03810-8.
8. Pukale, P., & Gupta, P. (2013). Analysis of end-to-end delay in vehicular networks. *International Journal of Science Research, 5*, 1122–1125.
9. Walters, J. P., Liang, Z., Shi, W., Chaudhary, V. (2007). Wireless sensor network security: A survey. In *Security in distributed, grid, mobile, and pervasive computing*: Auerbach Publications, pp. 367–409.
10. Liu, K., Deng, J., Varshney, P. K., & Balakrishnan, K. (2007). An acknowledgment-based approach for the detection of routing misbehavior in MANETs. *IEEE Transactions on Mobile Computing, 6*(5), 536–550.
11. Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials, 15*(4), 2046–2069.
12. Boukerche, A., Oliveira, H. A., Nakamura, E. F., & Loureiro, A. A. (2008). Vehicular ad hoc networks: A new challenge for localization-based systems. *Computer communications, 31*(12), 2838–2849.
13. Sarigiannidis, P., Karapistoli, E., & Economides, A. A. (2015). "Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information. *Expert Systems with Applications, 42*(21), 7560–7572.
14. Ogonji, M. M., Okeyo, G., & Wafula, J. M. (2020). A survey on privacy and security of Internet of Things. *Computer Science Review, 38*, 100312.
15. Sefati, S. S., & Tabrizi, S. G. (2021). Cluster head selection and routing protocol for wireless sensor networks (WSNs) based on software-defined network (SDN) via game of theory. *Journal of Electrical and Electronic Engineering, 9*(4), 100–115.
16. Park, P., Di Marco, P., Nah, J., & Fischione, C. (2020). Wireless avionics intracommunications: A survey of benefits, challenges, and solutions. *IEEE Internet of Things Journal, 8*(10), 7745–7767.
17. Sefati, S., Abdi, M., & Ghaffari, A. (2021). Cluster-based data transmission scheme in wireless sensor networks using black hole and ant colony algorithms. *International Journal of Communication Systems, 34*(9), e4768. https://doi.org/10.1002/dac.4768
18. Sengan, S., Subramaniyaswamy, V., Nair, S. K., Indragandhi, V., Manikandan, J., & Ravi, L. (2020). Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public data-smart network. *Future Generation Computer Systems, 112*, 724–737.
19. Verma, K., Hasbullah, H., & Kumar, A. (2013). Prevention of DoS attacks in VANET. *Wireless personal communications, 73*(1), 95–126.
20. 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 technique. *IEEE Access, 6*, 47258–47267.
21. Yu, B., Xu, C.-Z., & Xiao, B. (2013). Detecting sybil attacks in VANETs. *Journal of Parallel and Distributed Computing, 73*(6), 746–756.
22. Chen, C.-L., Chang, C., Chang, C.-H., & Wang, Y.-F. (2013). A secure ambulance communication protocol for VANET. *Wireless personal communications, 73*(3), 1187–1213.

23. Fogue, M., et al. (2014). Securing warning message dissemination in VANETs using cooperative neighbor position verification. *IEEE Transactions on Vehicular Technology, 64*(6), 2538–2550.
24. Jamshidi, M., Zangeneh, E., Esnaashari, M., Darwesh, A. M., & Meybodi, M. R. (2019). A novel model of sybil attack in cluster-based wireless sensor networks and propose a distributed algorithm to defend it. *Wireless Personal Communications, 105*(1), 145–173.
25. Liang, J., Chen, J., Zhu, Y., & Yu, R. (2019). A novel Intrusion Detection System for Vehicular Ad Hoc Networks (VANETs) based on differences of traffic flow and position. *Applied Soft Computing, 75*, 712–727.
26. Cunha, F., et al. (2016). Data communication in VANETs: Protocols, applications and challenges. *Ad Hoc Networks, 44*, 90–103.
27. Sefati, S. S., Navimipour, N. J. (2021). A QoS-aware service composition mechanism in the Internet of things using a hidden Markov model-based optimization algorithm. *IEEE Internet of Things Journal*, https://doi.org/10.1109/JIOT.2021.3074499.
28. Liu, J., Yang, W., Zhang, J., & Yang, C. (2020). Detecting false messages in vehicular ad hoc networks based on a traffic flow model. *International Journal of Distributed Sensor Networks, 16*(2), 1550147720906390.
29. Rajadurai, H., & Gandhi, U. D. (2020). Fuzzy based collaborative verification system for Sybil attack detection in MANET. *Wireless Personal Communications, 110*(4), 2179–2193.
30. Barnwal, R. P., Ghosh, S.K. (2012). Heartbeat message based misbehavior detection scheme for vehicular ad-hoc networks. In *2012 International Conference on Connected Vehicles and Expo (ICCVE)*: IEEE, pp. 29–34.

Seyed Salar Sefati received his B.Sc. in software computer engineering from the Institute of Higher Education Roshdiyeh in 2018; also, he received his M.Sc. degree from Islamic Azad University, in 2020. He is the top 3 students among the 130 students in master's degree. He is currently pursuing a Ph.D. degree at the University Politehnica of Bucharest (UPB) and researching in Ultra-Reliable Low-Latency Communications (URLLC) services in the Internet of Things (IoT).

Sara Ghiasi Tabrizi is graduated M.Sc. of information technology in [2015]-[2017] in Islamic Azad University her thesis was Data storage based on genetic algorithm in wireless sensor networks to reduce access time. She is researching about Internet of things, Cloud computing and Wireless sensor networks. Sara's skills in web programming, C# programming language, Bootstrap and access and SQL server databases. She also has 6 years' experience of security solutions and time attendance services.