International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 27, No. 4, August, 2022, pp. 605-611
Journal homepage: http://iieta.org/journals/isi

Sybil Attack Detection in VANET Using Machine Learning Approach

Sireesha Kakulla*, Srinivas Malladi

Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram 522502, A.P., India

Corresponding Author Email: sireeshakcs@gmail.com

https://doi.org/10.18280/isi.270410

Received: 17 June 2022
Accepted: 30 July 2022

Keywords:
sybil attack, Vehicular Ad-hoc Network (VANET), network security, network simulator

ABSTRACT

VANET (Vehicular Ad-hoc Network) is a subclass of MANET in which many cars can connect with one another via node to node or equipment erected on the side of the road. However, due to the adaptability of centres and the unexpected trade in geography, there may be opportunities for attacks in VANET. One of the ostensible assaults is the Sybil attack, in which the attacker fabricates unequivocally unique equal personalities to undermine the value of VANET. Sybil creates fictitious identities inside the community as well in order to sabotage attempts to mediate conversations between community nodes. Sybil assaults have an impact on carrier transportation in relation to things like traffic congestion, road safety, and multimedia entertainment. VANETs therefore announce a security mechanism to protect you from Sybil attacks. In this regard, this work puts forth the SDTC method, which completely relies on machine learning techniques to prevent Sybil assaults in VANETs. In order to reduce identification time, increase detection accuracy, and enhance scalability, the SDTC (Sybil node detecting the use of Classification) mechanism uses a few vehicle-specific Extreme Learning Machine (ELM) features. The results suggest that SDTC is a suitable strategy to reduce Sybil assaults and sustain provider service in VANETs.

1. INTRODUCTION

With new improvements in network geography and patterns, VANET is of great interest to experts and researchers. The Vehicular Ad-hoc Network (VANET) is the shadow of mobile ad hoc networks and has the potential to improve the welfare of travelers through vehicle-to-vehicle communication [1]. Portable ad hoc networks (MANETs) provide communication between standby devices. These gadgets provide communication between high-speed moving vehicles with no developments that are underdeveloped or violate the VANET standard layout [2]. Every year, in the natural process of things that will surely develop, so many vehicles have hit the streets. It causes street traffic that wastes time, cash, oil-based goods and more. The government is pouring more money to build more and more roads and wipe out the site by declaring that the current roads cannot support the generated traffic. There are answers to this many questions, including VANET. VANET helps establish communication between vehicles and further develop road traffic. Before that, of course, the vehicle collects traffic data and the driver makes choices based on that data.

VANET is a procedure to think about wise vehicle frameworks (ITS) considering the clever vehicle framework (ITS), considering the IEEE 802.11p norm for Wireless admittance to the Vehicle Environment (WAVE). VANET License Vehicles guarantee dependably in a room with no present establishment. In order to provide this type of help Banett, the VANET system's target destination that provides different organizations that can handle explorer, driving assistance, infotainment, transport policies, etc., requires accurate and happy data transfer. Information is sent in a vehicle (compact center) and a nearby stationary road (RSU). VANET interfaces vehicles that falls in the range of 100 to 500 meters and do not connect to different vehicles if the vehicle does not exist. Basically, the base consists of, for example, two types of correspondence.

1) Communication of a vehicle link (V2V). 2) Riding communication (V2i). Vehicle Conductor (V2V) Vehicle Correspondence is self-organizing because it does not require a framework for response. The scope of this organization is eventually 500 meters from the topographic position of the initiator car. Vehicles in this range can benefit from different vehicles with different vehicles with different vehicles in the organization. V2V shares vehicles in line about vehicle numbers, vehicle numbers, and prospect vehicles. In the opposite vehicle and factory (V2I), V2i response is absolutely to the present foundation, such as the Road (RSU).

V2I Communications RSUs communicate with vehicles to convey in-vehicle messages, road conditions, nearby accommodations, and internet access to the network. Figure 1: The VANET architecture gives an overview of VANET and the management it provides. Recognizing that vehicle development at VANET is very fast, the power of vehicle association and separation is so high that the region is constantly changing. In the meantime, there is an ideal opportunity for an attacker to track the organization as the topology changes. Therefore, security is also a central and urgent topic for VANET, and it is important to sort out and eliminate potential attacks. Initially, VANET is a remote organization, so it captures all the security risks of the remote organization. In addition, vehicle development at VANET is progressing and there are so many opportunities for attacks at the time of delivery that productive telecommunications vehicles will continue to move between regions. Various types of production attacks have been carried out and planned [3]. Attacks were analyzed based on vehicle speed, number of collisions, and percentage of time the luggage was carried. Gu et al. [4] uses scope rundown to recognize and distinguish Sybil Hub. This plan shows that if an adjacent hub is monitoring a vengeful hub for a long period of time, that hub will be recognized as a Sybil hub, but the drawbacks of this plan are very complex. It was time consuming. The review of VANET rules has been completed [5] on rules for unicast, multicast, geo cast, movie cast, and broadcast. A VANET route-based system has been proposed to guide the driver step by step. This framework helps to calculate a better course in real road conditions. Developers have proposed a framework model that uses the dynamic age will method to constrain and detect the Sybil hub. By developers [6], VANET vehicles are being studied to be mediated via RSUs using focal and street side servers. Correspondence can be vehicle-to-vehicle (V2V) or vehicle-to-vehicle (V2R). Grover et al. [7] proposed a common key management scheme that takes precedence over the mediated key management framework. Of course, this structure allows you to fill the vehicle without using RSUs. The message transmission is terminated by the RSU. An electronic crisis brake light system has been proposed by the developer, which alerts the outside of the vehicle and about weather patterns, and V2V compliance is used to spread the warning message to the vehicle. A decentralized, constrained approach has been proposed by the developer to identify Sybil hubs on the road. By focusing on signal strength, two calculations have been proposed for location checking and Sybil attack identification. Reproductions were made to examine the proposed plot. Eziama et al. [8] proposed Sybil Hub.

2. RELATED WORKS

2.1 Classification of attackers

In this part, we arranged the assailants in light of its way of behaving, nature and proficiency. Proficiency of all assaults relies upon the limit of assailant. Thusly, prior to examining assaults it is crucial for have some familiarity with the kind of aggressors as displayed in Figure 1.

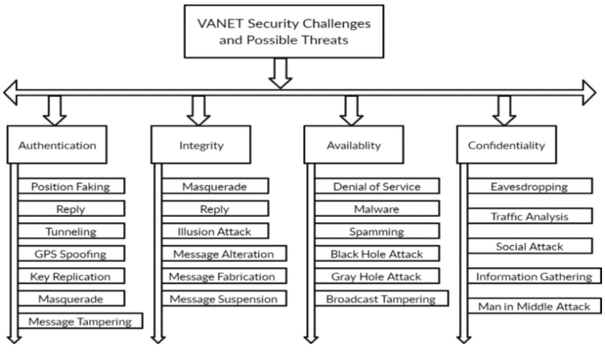

Figure 1. Sybil attack using VANET

2.2 Active vs. passive

A few assailants send or get no message on the organization; however, they snoop on the remote organization to acquire information.

2.3 Local vs. extended

Neighbourhood Attackers send-off assault of restricted scope and in restricted control local/region. Meanwhile, assailants of expanded class control a few elements, which are appropriated across entire organization. Stretched out class assailants can possibly corrupt the presentation of the organization or shut down the whole organization [9].

2.4 Sybil attack

Since VANET works in a remote climate, it is entirely defenceless against many kinds of safety assaults. The one of a kind sort of VANET adds extra weaknesses and intricacy in making secure organizations. There are numerous potential dangers to VANET; however, this report centres on the Sybil assault, which is the wellspring of numerous security dangers. Sybil assaults were first presented and portrayed by Douceur with regards to Peer to Peer networks. Sybil assaults are a digital protection danger. Forge new IDs or steal vehicle IDs online to impersonate multiple legitimate IDs as malicious vehicles. Attackers steal the IDs of other vehicles by eavesdropping on broadcast messages. This is because the vehicle is inherently mobile, the network density changes dynamically, and the network topology also changes dynamically, so the vehicle keeps communicating with other vehicles and updates the routing table. Attackers can use these properties to force a Sybil attack through a vehicle on the network, creating the illusion that there are multiple legitimate vehicles on the network using machine learning shown in Figure 2.

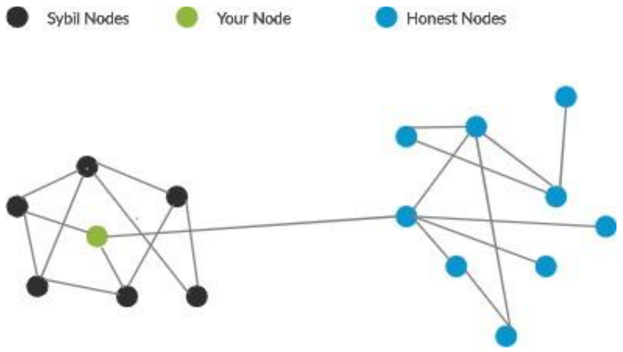

Figure 2. Sybil attack

Example: If a vehicle in a lane slows down significantly and sends a warning message. The recipient of the message will reply to this message and resend it [10]. However, if Sybil vehicles are present, they may refuse to respond and communicate (DOS attack). This upsets the genuine work of the association, can cause significant mishaps on the roadway and increment the quantity of passings. Also, Sybil vehicles inside the association might compel an assault on the vehicle or association.

Gu et al. [2-4] presented three amazing Sybil assault detection tactics in urban contexts, each of which can be fully dependent on the movement styles of automobiles. These strategies were introduced in urban environments. The mobility pattern can be symbolically represented by making use of the eigenvalues of a conduction matrix. Gu et al. utilized the Mlbis Distance Distance as a means of grading the degree of similarity across vehicle patterns, which made it possible to identify Sybil nodes. Later on, Gu et al. offered a solution for the identification of Sybil by classifying automobile nodes and differentiating them from Sybil nodes with the assistance of kNN Classification and Support Vector Machine (SVM) algorithms, respectively. This allowed the paper writers to determine which nodes were automobiles and which Sybil nodes were. In spite of the notable well-known performance that these methods provided, they posed three risks: I the general overall performance was tested in low-traffic situations (constrained automobile density); (ii) the runtime complexity was excessive; and (iii) the simplest rational model attacks were taken into consideration.

With the purpose of determining a relationship between Sybil nodes, Reddy et al. Developed a Sybil attack detection method for VANETs that is based completely on Infrastructure Observation-based totally Total Affinity Computation (IOAC). The provided approach makes use of the RSU to steer the monitoring of changes in the moving dynamics between vehicles when the following conditions occur: (1) vehicles travelling through several RSUs at the same time; and (2) in the context of notable RSUs, remarkable identities (IDs). As a consequence of this, and due to the fact that it employs a smooth identity mechanism, this method endeavors to synchronize data between RSUs (the car ID). The performance and scalability of the proposed method on VANETs were both put in peril as a result of these data.

A method for determining Sybil attacks was developed by Reddy et al. [5], and it is frequently dependent on the current state of encrypted virtual signatures. The suggested method employs these signatures as hash attributes to establish a do not forget issue for several of the speaking entities. This makes it possible to check the car node's existence. This method, on the other hand, does not bring to mind the mobility behavior of the car nodes and, as a result, restricts identity in settings with an excessive amount of movement and density.

Grover et al. [7] suggested a mischievous detection system that makes use of physical and behavioral statistics for every vehicle node. This information includes unique node velocity, acquired signal strength (RSS), variety of packets transmitted, variety of packets deleted, and many more. By utilizing binary and multi-Class categories, this protection architecture aims to differentiate between malicious nodes and legal nodes [11], because this framework is susceptible to not rare mischief, it does not engage in Sybil assaults any longer [12]. As a result, it has a reduced chance of coming across this form of attack and, as an end result, a better chance of mitigating its effects and remaining safe from it [13].

Eziama et al. presented node operation for safety and protection, using a reliability assessment version and a Bayesian Neural Network that integrates deep learning in addition to probabilistic modelling to become aware of authentic and rogue nodes in the network. This allows the network to become aware of authentic and rogue nodes. In spite of the approach for learning about the device, the paper writers are unable to recall the movement pattern of the car nodes, which demonstrates that there is a lack of flexibility.

Engaged short-lived pseudo certificates to ensure privacy and anonymity for vehicle nodes while also reducing the possibility of Sybil attacks. On a regular basis, each vehicle node broadcasts to its community a list of suspected Sybil nodes. Furthermore, a temporary identifying mechanism is employed to reduce the risk of the assault while still providing the consumer with privacy and anonymity. In Table 1 shows as a result [14], Sybil node identification occurs concurrently with the attacker profiting from a vehicle's transient identity, which renders it unusable after expiration. However, because this approach is dependent on the presence of the auto nodes and does not take into account automobile behavior, it is impeded by excessive mobility and topological disruption circumstances [15].

Table 1. Literature survey

Reference	Methods	Disadvantages
[2]	SVM	Complexity in terms of the computations required
[3]	Mlbis Distance	Sybil attacks because she only takes into account the logical model.
[4]	KNN	Extreme computational difficulty
[5]	Digital Signature Encryption	No evaluation in high density scenarios
[7]	Binary and Multi-class Classification	No estimation of node behavior
[8]	Bayesian Neural Network	No estimation of node behavior
[9]	IOAC	Low scalability and a passive technique for identification
[10]	Dynamic Certification and Neighbor-hood Lists	There is no estimation of the behavior of the nodes.
SDTC (proposed)	Extreme Learning Machine	No evaluation in low density scenarios

Most existing methods for identifying Sybil attacks estimate the location of neighboring nodes using Received Signal Strength Indication (RSSI) and compare it to the geographic role indicated in the beacon statistics [16]. As a substitute, several solutions rely on a data-theoretic framework and are not scalable even when the density of vehicle nodes is high. To the best of our knowledge, no previous research has focused on the detection of Sybil attacks in VANETs by utilizing Extreme Machine Learning to choose out Sybil nodes based on motion similarity definition from data gathered via backend stations, which is the focus of this study [17].

3. PROPOSED METHODOLOGY

One of the most essential responsibilities for ensuring the security, integrity, and privacy of VANETs is Sybil assault detection. The identification of Sybil assaults should not interfere with the normal operation of VANETs, nor should it impede carrier shipping for auto nodes [18]. As a result, solutions for Sybil attack detection must be rapid, scalable, and low in complexity. This paper provides a method called SDTC to meet this need in this context.

The SDTC method defines a motion matrix based on the mobility patterns of vehicular nodes. This motion matrix is used in an Extreme Learning Machine (ELM) method to evaluate the mobility of true vehicle nodes in front of Sybil node displacement inaccuracy, allowing Sybil node detection. As a result, the movement matrix is explained first, followed by the ELM approach. Following that, the SDTC requirements and implementation strategies are defined: Section 3A outlines the movement definition matrix, Section 3B describes the ELM method implementation and record processing, and Section 3C introduces the Sybil attack detection methodology.

A. Movement matrix defined

Beacons and Context Awareness Messages (CAMs) are the mechanism by which a vehicle node in a VANET routinely communicates with its neighbors in order to provide the latter with information regarding the location of the vehicles that are located in close proximity to it. CAMs are often provided (in broadcast) at a rate of one per hundred millisecond via a single-hop connection that can span a distance of at least one kilometer [19]. The contents of the communications include not only the identities of the nodes, but also their positions, times, speeds, and accelerations, in addition to information regarding mobility and context. In addition, the information that was documented is accessible to the base stations in the internet-paintings region regardless of the method that was utilized (as an instance, RSUs, LTE towers, and many others). This information may be utilized to infer the behavior of man or woman vehicle nodes and the VANET environment as a whole, making it an extremely useful tool for identifying inappropriate behavior in VANETs [20].

As a consequence of this, the SDTC mechanism gathers information regarding the vehicle's node inside the side base stations and uses this information to construct a motion matrix. The car mobility pattern description can be thought of as a collection of facts describing the movement of an automobile node over the course of a particular time period [21]. The motion matrix of a given vehicle node, Mi, represents this car mobility pattern description. [Citation needed] In addition, the acceleration version that should be used between each sequential instance is determined for each vehicle.

The sample taken by a vehicle node at time t is represented as a vector with the following five details:

$V_{i,t}$ is equal to ($m_{t,1}$, $m_{t,2}$, $m_{t,3}$, m_t, four, $m_{t,5}$), where $m_{t,1}$ is the time of the automobile, $m_{t,2}$ is the location of the automobile, $m_{t,3}$ is the speed of the automobile, $m_{t,4}$ is the acceleration of the automobile, and $m_{t,5}$ is the variation in the acceleration of the automobile. The vectors are dependent on a matrix that specifies the route that they will take across the network during a given time period (beginning from 1 to n, as laid out in Equation 1).

$$M_i = \begin{bmatrix} m1,1 & m1,2 & m1,3 \ldots. \\ m2,1 & m2,2 & m2,3 \ldots. \\ m3,1 & m3,2 & m3,3 \ldots.. \end{bmatrix} \tag{1}$$

As a direct consequence of this, the SDTC approach establishes a rigid and inflexible $M=M_1 \ldots M_i$, M_k of motion inside of a VANET that comprises desirably positioned vehicle nodes. This set illustrates the motion pattern of the VANET, which may be thought of as an international picture of how the environment behaves. M serves as the foundation for the Sybil node identity strategy that is implemented within the following method.

B. Data processing

The Artificial Neural Network (ANN) is a broad artificial intelligence mathematical device that is utilized for prediction, sample popularity, and type. However, this traditional device is modern, and it has issues with stopping standards, studying fee, minimal neighborhood, and over-tuning. A method of trading that was given the name Extreme Learning Machine (ELM) was developed as a reaction to these limits. Within the ELM, the input weights and hidden biases are chosen at random, whilst the output weights are computed analytically by the use of the Moore-Penrose generalized inverse. This method enables you to forget about the difficulty as a linear tool, which subsequently enables you to carry out a generalized inverse operation on the output matrices of the hidden layer. As a consequence of this, ELM is more rapid and less complicated than fashionable feed earlier learning algorithms, and it gets rid of the problems that have been discussed above. When seen in this light, ELM is an excellent method for use in the SDTC mechanism for Sybil attack detection since it enables increased detection accuracy and scalability in high-density situations. Following the M specification of the set matrix of activities contained inside the SDTC mechanism, the ELM is utilized to determine the similarity of mobility patterns of actual nodes, as is illustrated further down in this section. In order to make use of ELM, it is necessary to process the data in a manner that will permit a reduction in the dimensionality of the data. This can be accomplished by computing the eigenvalues of each matrix of motion $M_1 \ldots M_i$, M_k in accordance with the procedures described in Algorithm 1.

C. Detecting Sybil node

This section demonstrates the SDTC mechanism in action by utilizing the ELM magnificence to locate Sybil nodes in VANETs. Figure 3 depicts the overall process that has been completed.

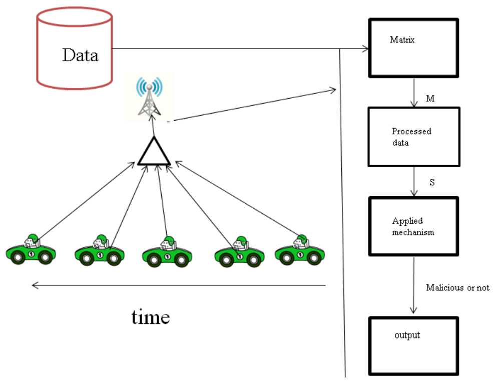

Figure 3. SDTC approach for Sybil node detection

3.1 Classification using machine learning approach

First, the statistics are gathered from the nodes representing the automobiles, and then the matrix of motion is presented, as described in the matrix movement 3A definition. After some time has passed, these records will be processed so that meaningful statistics can be gleaned regarding the mobility patterns of the car nodes. Data Processing, 3B, in which the matrix is represented by making use of the two eigenvalues with an excessive amount of power. Following completion of this process, the ELM classifier will take as its input the pair of eigenvalues that are the most pertinent to the situation. The ELM classifier is well-versed in the utilization of the eigenvalues of each node in the VANET. This enables it to not only determine the behavior of the vehicle but also become aware of misbehaving motors, which may be Sybil nodes. Epoch is the name that is given to each individual educational cycle that is finished using the ELM model. Throughout the course of the experiments, a scattering of educational epochs was chosen to represent the ELM version. As a consequence of this, in the course of the model tuning process, the variety of Epochs became gradually increased so as to supply a better fitting and evaluation of the SDTC mechanism. For instance, after a certain number of epochs, say 100, the ELM version has not yet converged to a minimum that is quite close. During the course of the trials, we looked at anywhere from one hundred to one thousand different Epochs times (greater details will be furnished in subsequent section, Results).

3.2 SDTC mechanism

The identification of Sybil attacks is one of the most essential duties that must be fulfilled in order to guarantee the security, privacy, and integrity of VANETs. It is now expected that the discovery of Sybil attacks would not impair ordinary VANET operations, nor should it change the manner in which services are made available to mobile nodes. It is important for replies to be concise, scalable, and occasionally ingenious if they are to be successful in thwarting Sybil attacks. This note hints at an SDTC strategy that can close this gap in this particular setting. A movement matrix that is frequently and mostly based on a sample of vehicular node mobility is displayed by the SDTC mechanism. This movement matrix is used in an Extreme Learning Machine (ELM) technique to compare the mobility of genuine automobile nodes against the incorrect displacement of Sybil nodes, which enables the identification of Sybil nodes to be determined.

3.3 Data approaching

The Data Processing Artificial Neural Network, more commonly referred to as an ANN, is a mathematical tool that is widely used for forecasting, sample popularity, and classification. On the other hand, this conventional strategy is just as challenging because to issues with pausing requirements, getting to know expenses, minimal neighbourhood, and over-tuning. An up-to-date method that is currently in use is known as the Extreme Learning Machine (ELM), and its development was precipitated by these limits [13]. Within the ELM, the doorway weights and hidden biases are chosen at random; nevertheless, the output weights are derived analytically with the use of the Moore-Penrose generalised inverse. If you use this strategy, it will likely be much less difficult for you to consider the challenge as a linear tool. This is particularly the case if you think about the application of a generalised inverse operation to the output matrices of the hidden layer. ELM is far faster and less complicated than the more modern feed forward mastering algorithms, and it eliminates the shortcomings that were discussed previously. As a consequence of this, ELM eliminates the problems that were mentioned earlier. Because it maximises detection accuracy and scalability in high-density situations, ELM is an excellent technique that should be employed within the SDTC mechanism for the purpose of detecting Sybil assaults. This is the setting in which we are having the ELM conversation. Following the derivation of the set matrix of moves M, the ELM is put to use within the SDTC mechanism to determine the degree to which the mobility patterns of actual nodes are comparable to one another, as the subsequent illustration will show [22]. The ELM was utilised in order to arrive at this conclusion.

3.4 Algorithm for SDTC

- This method calculates the mean of each column of M_i matrix $a_k = \sum_{p=1}^{n} \left(m_{p,k}\right) /n$;
- Subtracts from each element of the respective column. $m_{p,k}= m_{p,k}-a_k$;
- The eigenvalues are calculated (Eigen) EG;
- $M_p^Q = M_{p*} M_p^T$;
- Represented by the Energy (E) of the eigenvalues, with the E that is greater than that of the other EG being taken into consideration.
- As a result of the guided information processing, data is collected from the Vehicle nodes, and a description of the movement matrix is provided.

This information is analyzed in order to extract useful information regarding the mobility pattern of the vehicle nodes, and the matrix is represented by means of the two excessive power eigenvalues (EG).

4. EXPERIMENTAL RESULTS

The SDTC approach that has been recommended is now being explored in order to find Sybil nodes that are present within the network. Numerous checks had been performed with the use of the SUMO simulator, the Sybil nodes era and detection method in Python, and the ELM Classification set of regulations in KERAS. All of them had been effective in producing the desired results. Every piece of this equipment has been put to use.

When we talk about accuracy, we typically refer to the proportion of the total number of right predictions to the total variety of input samples as our suggested metric. The fraction of Sybil nodes that are contained within the VANET has increased, as can be seen in the Table 2 below. This is due to the fact that there are now more automobiles than there were previously. The Mechanism's accuracy has also increased.

Table 2. Output network simulator parameters

Parameter	Value
Version	SUMO 1.2.0 simulator real world
Speed of node	10 - 100 km/h
Width Area	2 lanes
Length Area	100m
Vehicles simulated	800
Output Time	200s
Number of passes (Epoch)	300 to 1000
OutputScenario	Manhattan Grid 4X4
Sybil Samples Percentage	1%,5%,10%,15%,20%

Utilizing a Confusion Matrix allows for the estimation of both a loss in accuracy as well as cross-entropy. It is feasible to evaluate the overall efficacy of classifiers by primarily focusing on the amount of times they get a classification right and the number of times they get it wrong. A table that presents the sort frequency for each beauty that is offered within the model is called the Confusion Matrix [23].

Concerning the Cross-entropy loss, it is a measurement that determines the effectiveness of the classifier, the output of which is a chance fee ranging from 0 to 1. In most cases, the Cross-entropy loss will get worse as the anticipated probability gets further and further away from the actual label. When seen in Figure 4, in this light, the total performance of the classifier is thought to be superior whenever there is a decrease in the price shows in Figure 5 and Figure 6.

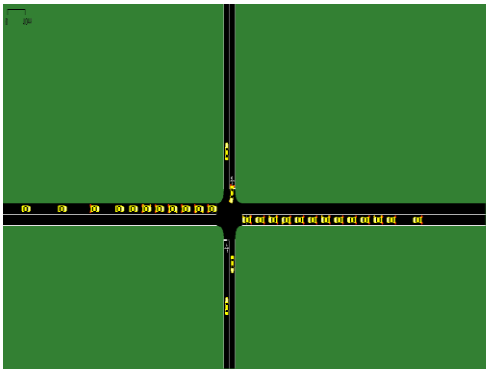

Figure 4. Sumo 1.2.0 environment with real world vehicles

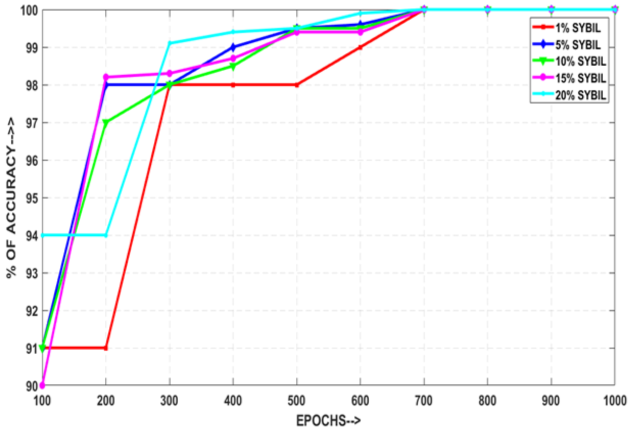

Figure 5. Simulation done for number of passes for detecting accuracy

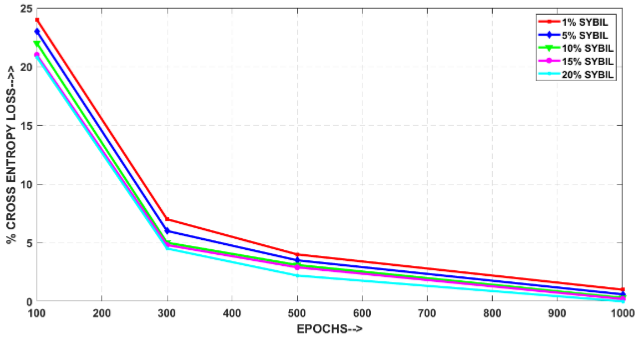

Figure 6. Simulation for number of passes for finding cross entropy

5. CONCLUSIONS

The vindictive hub is intended to go about as a Sybil aggressor. No bundle misfortune was noticed assuming the framework had no aggressors, however including the Sybil assailants, practically all parcels were dropped by the assailants. As the quantity of hubs builds, the location rate increments. The heap size on the DMV grows larger as the number of attackers that are currently contained within the framework grows. As the number of hubs contained inside the framework increases, the number of misleading negatives decreases. As a result of its open status quo, the Vehicular Ad-hoc Network (VANET) is vulnerable to a variety of security threats, including Sybil attacks, and should be treated with caution. Within the scope of this work, we have suggested an approach that makes use of digital signatures to identify Sybil assaults [24]. Cars, Roadside Units (RSUs), and the Department of Motor Vehicles are all brought together by the needed shape (DMV). In the game Sybil assault, a hazardous centre known as the Sybil attacker is responsible for illegally making certain a large number of characters who are referred to as Sybil centres. The findings demonstrated that the deployment of the SDTC in VANETS demonstrated a high detection rate with a significantly reduced number of errors rates. These descriptions demonstrate the benefits that the SDTC technique offers in comparison to the solution that is currently available for detecting Sybil assaults. As potential improvements for the near future, we might think about combining the ELM approach with several other artificial intelligence and deep learning algorithms.

REFERENCES

[1] Li, J., Lu, H., Guizani, M. (2014). ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs. IEEE Transactions on Parallel and Distributed Systems, 26(4): 938-948. https://doi.org/10.1109/TPDS.2014.2308215

[2] Gu, P., Khatoun, R., Begriche, Y., Serhrouchni, A. (2017). Support vector machine (SVM) based sybil attack detection in vehicular networks. In 2017 IEEE Wireless communications and networking conference (WCNC), San Francisco, CA, USA, pp. 1-6. https://doi.org/10.1109/WCNC.2017.7925783

[3] Gu, P., Khatoun, R., Begriche, Y., Serhrouchni, A. (20216). Vehicle driving pattern based sybil attack detection. In 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Sydney, NSW, Australia, pp. 1282-1288. https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0182

[4] Gu, P., Khatoun, R., Begriche, Y., Serhrouchni, A. (2017). k-Nearest neighbours classification based sybil attack detection in vehicular networks. In 2017 Third International Conference on Mobile and Secure Services (MobiSecServ), Miami Beach, FL, USA, pp. 1-6. https://doi.org/10.1109/MOBISECSERV.2017.7886565

[5] Reddy, D.S., Bapuji, V., Govardhan, A., Sarma, S.S. V.N. (2017). Sybil attack detection technique using session key certificate in vehicular ad hoc networks. In 2017 international conference on algorithms, methodology, models and applications in emerging technologies (ICAMMAET), Chennai, pp. 1-5. https://doi.org/10.1109/ICAMMAET.2017.8186733

[6] Mekliche, K., Moussaoui, S. (2013). L-P2DSA: Location-based privacy-preserving detection of Sybil attacks. In 2013 11th International Symposium on Programming and Systems (ISPS), Algiers, Algeria, pp. 187-192. https://doi.org/10.1109/ISPS.2013.6581485

[7] Grover, J., Prajapati, N.K., Laxmi, V., Gaur, M.S. (2011). Machine learning approach for multiple misbehavior detection in VANET. In International Conference on Advances in Computing and Communications, pp. 644-653. https://doi.org/10.1007/978-3-642-22720-2_68

[8] Eziama, E., Tepe, K., Balador, A., Nwizege, K.S., Jaimes, L.M. (2018). Malicious node detection in vehicular ad-hoc network using machine learning and deep learning. In 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, pp. 1-6. https://doi.org/10.1109/GLOCOMW.2018.8644127

[9] Hamed, H., Keshavarz-Haddad, A., Haghighi, S.G. (2018). Sybil attack detection in urban VANETs based on RSU support. In Electrical Engineering (ICEE), Iranian Conference on, Mashhad, Iran, pp. 602-606. https://doi.org/10.1109/ICEE.2018.8472629

[10] Sharma, A.K., Saroj, S.K., Chauhan, S.K., Saini, S.K. (2016). Sybil attack prevention and detection in vehicular ad hoc network. In 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, pp. 594-599. https://doi.org/10.1109/CCAA.2016.7813790

[11] Park, S., Aslam, B., Turgut, D., Zou, C.C. (2009). Defense against sybil attack in vehicular ad hoc network based on roadside unit support. In MILCOM 2009-2009 IEEE Military Communications Conference, Boston, MA, USA, pp. 1-7. https://doi.org/10.1109/MILCOM.2009.5379844

[12] Jin, D., Song, J. (2014). A traffic flow theory aided physical measurement-based sybil nodes detection mechanism in vehicular ad-hoc networks. In 2014 IEEE/ACIS 13th International Conference on Computer and Information Science (ICIS), Taiyuan, China, pp. 281-286. https://doi.org/10.1109/ICIS.2014.6912147

[13] Douceur, J.R. (2002). The sybil attack. International Workshop on Peer-to-Peer Systems, 2429: 251-260. https://doi.org/10.1007/3-540-45748-8_24

[14] Xiao, B., Yu, B., Gao, C. (2006). Detection and localization of sybil nodes in VANETs. In Proceedings of the 2006 Workshop on Dependability Issues in Wireless AD Hoc Networks and Sensor Networks, pp. 1-8. https://doi.org/10.1145/1160972.1160974

[15] Grover, J., Gaur, M.S., Laxmi, V. (2010). A novel defense mechanism against sybil attacks in VANET. In Proceedings of the 3rd International Conference on Security of Information and Networks, pp. 249-255. https://doi.org/10.1145/1854099.1854150

[16] Grover, J., Gaur, M.S., Laxmi, V., Prajapati, N.K. (2011). A sybil attack detection approach using neighboring vehicles in VANET. In Proceedings of the 4th International Conference on Security of Information and Networks, pp. 151-158. https://doi.org/10.1145/2070425.2070450

[17] Hao, Y., Tang, J., Cheng, Y. (2011). Cooperative Sybil attack detection for position based applications in privacy preserved VANETs. In 2011 IEEE Global Telecommunications Conference-GLOBECOM 2011, Houston, TX, USA, pp. 1-5. https://doi.org/10.1109/GLOCOM.2011.6134242

[18] 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. https://doi.org/10.1109/JSAC.2011.110308

[19] Kafil, P., Fathy, M., Lighvan, M.Z. (2012). Modeling Sybil attacker behavior in VANETs. In 2012 9th International ISC Conference on Information Security and Cryptology, Tabriz, Iran, pp. 162-168. https://doi.org/10.1109/ISCISC.2012.6408215

[20] Triki, B., Rekhis, S., Chammem, M., Boudriga, N. (2013). A privacy preserving solution for the protection against sybil attacks in vehicular AD hoc networks. In 6th Joint IFIP Wireless and Mobile Networking Conference (WMNC), Dubai, United Arab Emirates, pp. 1-8. https://doi.org/10.1109/WMNC.2013.6549051

[21] Kamel, J., Jemaa, I.B., Kaiser, A., Urien, P. (2018). Misbehavior reporting protocol for c-its. In 2018 IEEE Vehicular Networking Conference (VNC), Taipei, Taiwan, pp. 1-4. https://doi.org/10.1109/VNC.2018.8628407

[22] Pouyan, A.A., Alimohammadi, M. (2014). Sybil attack detection in vehicular networks. Computer Science and Information Technology, 2(4): 197-202. https://doi.org/10.13189/csit.2014.020403

[23] Hao, Y., Tang, J., Cheng, Y. (2011). Cooperative Sybil attack detection for position based applications in privacy preserved VANETs. In 2011 IEEE Global Telecommunications Conference-GLOBECOM 2011, pp. 1-5. https://doi.org/10.1109/GLOCOM.2011.6134242

[24] Ghaleb, F.A., Zainal, A., Rassam, M.A., Mohammed, F. (2017). An effective misbehavior detection model using artificial neural network for vehicular ad hoc network applications. In 2017 IEEE conference on application, information and network security (AINS), Miri, Malaysia, pp. 13-18. https://doi.org/10.1109/AINS.2017.8270417