Journal of Positive School Psychology
2022, Vol.6, No.3, 7743 - 7756

http://journalppw.com

An Improved Security Algorithm for VANET using Machine Learning

Heena Khanna[1], Manmohan Sharma[2]

[1,2]Lovely Professional University, Phagwara, Punjab, INDIA

Abstract:

Vehicular Ad-Hoc Networks (VANETs) have become a fascinating research area over the last decade due to the increasing number of Vehicles on road. A secure Intelligent Transportation System (ITS) ensures the safety of the passengers and the driver nevertheless the dynamic characteristics of it make it a challenging area in terms of real time implementation. This paper proposes an improved security algorithm for VANET, which is able to deal with the threats like Denial of Service Attack (DoS), Sybil and Replay. The proposed work uses Enhanced K-Mean method to create the clusters for various attacks and a hybrid approach using Support Vector Machine (SVM) and Feed-forward back propagation is used to test the classifier for its accuracy. The results show a significant improvement in terms of Throughput, Jitter and PDR. Finally, we highlight future direction and some open issues for further exploration.

Keywords: V2V, VANET, ML, DDOS

1. INTRODUCTION

As the communication technology has been expanding more than ever before, the need for the secure transmission of messages is increasing many folds every day. With the number of devices becoming enormous day after the other, the risk of potential threats to attack the network is requiring an edge over the data transmission itself. There is a variety of the networks being created for various purposes and all of them are dealing with one or the other type of attacks. An Ad Hoc Network created for the message transmission over Vehicles running on the road is termed as **VANET** [1]**.** The applications based on VANETs exchange safety and traffic related messages with the vehicles running on the road. VANET is a special type of Mobile Ad Hoc Network (MANET). High number of nodes (vehicles) and continuous mobility are two major characteristics of VANET. A secure VANET can ensure a safe ITS. According to World Health Organisation, the eighth leading reason of deaths in the World is nothing but Road Accidents [2]. This gives a major motivation to the researchers for exploring VANET and the challenges associated with it. A secure VANET is certainly going to bring a shift to the increasing number of Fatalities related to road accidents.

Despite of all the progress in the field of VANET, the existing threats are making it difficult to have a complete ITS enabled world. Therefore, in this paper we will focus on identifying and exploring various attacks and their impact on the network. In later sections of the paper, we propose a methodology to segregate various types of attacks on the basis of their features and behaviour. Towards the end, some open issues are discussed for the future researchers.

This paper categorises various threats according to the category they fall in and then applies Machine Learning to provide a secure VANET algorithm. In Section 2 & 3, a list of protocols and approaches proposed to overcome various threats has been discussed. In Section 4, Machine Learning and various algorithms are discussed under it. A brief analysis has been depicted for the algorithms and proposals made by previous researchers under VANET using Machine Learning have been listed. Section 5 talks about the motivation behind this work and the proposed methodology. Here, we will differentiate between various attacks to deal with them better. A method is proposed to categorise the attacks on the basis of their behaviour in this section. In Section 6, the proposed architecture is compared with the existing algorithm and improved results are shared. The section is culminated with the conclusion of this paper and finally in Section 7 we have enlisted some of the open research areas to be explored by future researchers.

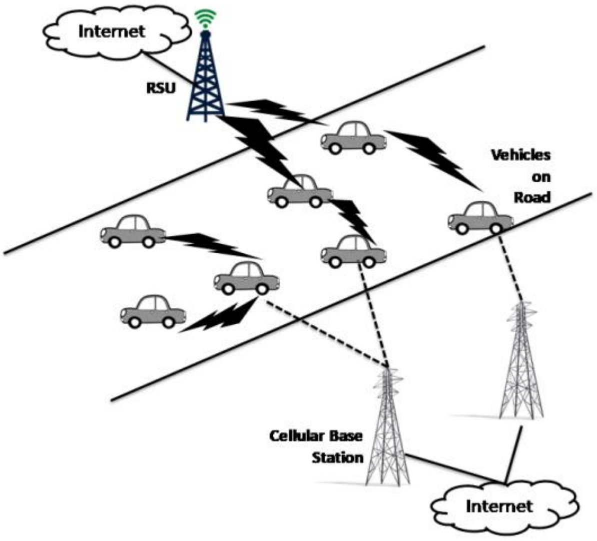


Figure 1VANET Architecture

2 Security Attributes

In this section we will discuss about some of the studies accomplished on exploring the security attributes over VANET and share a contrast amongst them. Before the discussion starts on the types of attacks, it is also important to understand various privacy and security requirements. As per, [3] [4]and [5] following are the major attributes for Security over VANETs.

i. **Availability**: At any point of time, the node should be available to transfer the data.

ii. **Authentication**: It refers to the surety that the data has been sent by a genuine vehicle.

iii. **Confidentiality**: It ensures that the information shared over the network is secure and a guarantee is given by the network that it will not share the data with unapproved users/vehicles.

iv. **Integrity**: Integrity means that the message reaches the receiver exactly as it is sent by the sender. No tampering is done with the message during the entire dissemination process.

v. **Non-Repudiation:** NR refers that the sender of the message does not deny the sending of the message, in case of an investigation. [6] proposed a cryptography based mechanism to ensure the Integrity and Non-Repudiation.

vi. **Scalability:** The network should have the ability to add as many numbers of vehicles as required for the smooth transfer of the important messages. For all the logistical reasons it will add on to the complexity of the system and the overall performance of the network may come down[7].

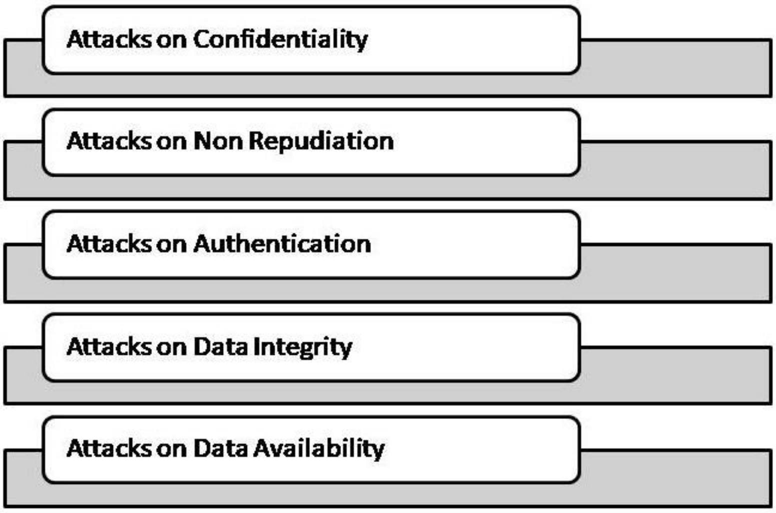

Attacks on Confidentiality
Attacks on Non Repudiation
Attacks on Authentication
Attacks on Data Integrity
Attacks on Data Availability

Figure 2 Attacks in VANET

In order to have a secure VANET it is important to understand the security concerns which are part and parcel of it. Further various types of attacks and the available approaches or protocols are conferred.

3 Categorisation of various attacks

In this section we introduce the attacks which are encountered over the VANET along with the proposed models corresponding to them. First let's understand various categorisation of the attacks [3] .

a. **Confidentiality** In order to ensure trustworthiness in the network, it must maintain a minimum threshold of the number of vehicles which approve that a said vehicle is genuine[8]**.**

   i. **Man in the Middle Attack (MiMA)** In this type of attack, the malicious node/vehicle comes in the middle of two vehicles communicating with each other and become a part of the network. After that the attacker tweaks the message and sends the incorrect message to the receiver. The solution to this type of attack is to generate a unique session key for every message so that even if the attacker grabs the message, in absence of the session key the main message cannot be tampered[3] [4][9].

   ii. **Eaves Dropping Attack** This is a variation to **MiMA** which attacks at Network Layer. Here the attacker silently listens to the message by obtaining the session key of any active communication. Due to the availability of Session Key, the message can be easily decrypted and hence tampered [5] [10].

   iii. **Traffic Analysis Attack** It is a Passive Attack which is an extension of Eaves Dropping Attack. In this attack, the attacker collects the messages and observes the pattern of the network to breach the flow of the Network [3].

b. **Non-Repudiation:** The intent of repudiation attacks is to cause delay and consume network bandwidth. Here, the attacking vehicle denies being the receiver or sender while acting one in the network.

c. **Integrity Attacks** This category of attacks comprises the ones where the message is tampered and does not reach the receiver as the original one.

i. **Replay Attack** This attack confuses the network by resending the old data over the period of time. It may result in some disastrous outcomes such as an impending collision. Time stamping is a potential solution to this type of attack [3] [5]

ii. **Masquerading Attack** As the name suggests it is an attack were the malicious vehicle pretends to be someone else. Techniques like Replay, Fabrication and Alteration are used to achieve the same and the network is used for a wrong cause. An example could be the attacker pretending to be an ambulance to get priority over the others. [3][4]

iii. Illusion Attack(ILA) All the state of affairs when the attacker sends a fake word of warning to the network regarding speed, accidents, jam etc. come under the Illusion Attack. [3][4]

d. Authentication

i. **Replication Attack** Also called as Node Replication Attack is when an unauthorised vehicle impersonates to be a genuine part of the network. It is done with a purpose to spared incorrect messages within the network [3] [11]

ii. **Spoofing Attack** Spoofing attacks are also called as GPS Spoofing Attacks. It is one of the major factors behind the fail of VANETs. In this attack, the malicious vehicle manoeuvres the received GPS signal within the VANET. This is a threatening situation as the location of the sender is overpowered by the attacker [5][12]

iii. **Tunnelling Attack (TA)** In this attack the attacker creates a fictional tunnel of its own within two nodes. This can completely compromise the VANET as the complete control is under the attacker and he/she can send , receive or steal any information within that tunnel without letting the other nodes know about the whole drill [3]

iv. **Sybil Attack (SA)** Under this attack, multiple identities of the same vehicle are generated in the network which gives an illusion of multiple vehicles. It can lead to a risky situation since the same vehicle can state to be at multiple locations and sending diverse messages [4] [13] [14]

v. **Wormhole Attack** Under Wormhole Attack, the mugger creates a tunnel with two or more malicious nodes and start transmitting the messages and broadcasting of unwanted messages. This way they take control over the network and get to delete the authentic messages as well[3][4]

vi. Impersonation Attack When a vehicle impersonates to be some other node which is trustworthy within the network or in other words when a vehicle hides its identity by showing to be someone else and sending messages on their behalf. [4] [14]

e. Availability

i. **DoS Attack** means Denial of Service Attack. In this the intruder attacks the network channel in order to cause the failure in packet transmission properly and timely. Here the attacker drags down the performance of the network by infusing a huge amount of fake packets, sometimes jams the network or drops the authentic packets. It is an active multilayer attack [13][15][16]. Black hole, Gray hole and Spamming are special cases of DoS Attack.

When the nodes start dropping the messages instead of forwarding them, it becomes Black Hole Attack. Whereas in Gray hole attack , the network layer is compromised to drop any and many number of packets. Further, in case of Spamming Attack the network is burdened with the excess of Spam Data Packets [3][17]

ii. **Greedy Behaviour Attack** It is a special type of Attack which is found in VANET where the vehicles become greedy and want to utilize the resources and misguides the fellow vehicles running on the road so that the greedy vehicle can get a clear path for itself. [18]

Attack	**Security Attribute**
Replication Attack	Authentication
Spoofing Attack	Authentication
Tunnelling Attack	Authentication
Sybil Attack	Authentication
Wormhole Attack	Authentication
Impersonation Attack	Authentication
DoS Attack	Availability
Black hole Attack	Availability
Gray hole Attack	Availability
Greedy Behaviour Attack	Availability
Man in the Middle Attack	Confidentiality, Integrity
Eaves Dropping Attack	Confidentiality , Integrity
Traffic Analysis Attack	Confidentiality
Masquerading Attack	Integrity
Replay Attack	Integrity, Confidentiality
Illusion Attack	Integrity
Repudiation Attack	Non-Repudiation

Figure 3 Categories of Attacks

4 Machine Learning and Types

Machine Learning helps the computer systems to analyse and find the insights observing the pattern and behaviour of the data over the period of time. This technology is revolutionary as it has given a new dimension to Computer Science as it enhances the capability of algorithms by themselves [19][20]. Machine learning can be broadly classified into three categories, namely, Supervised, Unsupervised and Reinforcement Learning.

A. **Supervised Learning:** Most of the algorithms fall under the category of Supervised Learning. As the name says the datasets hereby are labelled i.e. the training set already has the class labels. Under Supervised Learning, the Learning Phase works on creating the rules so that the future data can be predicted for their class labels according the Rules/Model defined.

There are further two categorisation of it on the basis of the data. The data with numerical labels comes under **Regression** whereas the Categorical ones come under the head of **Classification.** Classification is a two way process distributed in Learning and Testing Phase. Some popular classifiers are Decision Trees, Bayesian Classifiers, K-Nearest Neighbours, Support Vector Machine(SVM) and Neural Networks[21][22][23] [24][25]

B. Unsupervised Learning: Learning model with class label works as a Supervisor which by any means is an effective way as it ensures the accuracy level of the classifiers. But finding a huge dataset with labels is not always possible and then Unsupervised Learning comes into existence. Under this the algorithms are left on their own for the discovery, as there is no teacher like in case of Supervised Learning. Clustering and Dimensionality Reduction are two representations. **Clustering** is the process of grouping the data with similar properties together. K-Means Clustering, Hierarchical Clustering , Spectrum Clustering and Dirichlet Process are some popular clustering algorithms [23][26][27] . **Dimensionality Reduction** is the second effective category of Unsupervised Learning. This focuses on reducing the high dimension data into the less dimension data. The focus of dimension reduction is to ensure that there is no data loss while reducing the attributes. Some popular algorithms under dimensionality reduction are Principal Component Analysis, Local Linear Embedding and Isometric Feature Metric. [28].

C. Reinforcement Learning: It works on the reward model which learns from the environment by observing the hit and trial methods. The overall structure of Reinforcement Learning is to focus upon maximizing the number of rewards aimed and achieved from the environment. The model used here is called Markov Decision Process (MDP) which works around action and reward mechanism[29]**.**

D. Deep Learning: It is an advanced field of Machine Leaning which may use Supervised, Unsupervised or Reinforcement Learning to incorporate the models. The concepts of Deep Learning have contributed highly in Natural Language Processing (NLP), Computer Vision and Speech Recognition. [1][19][30]

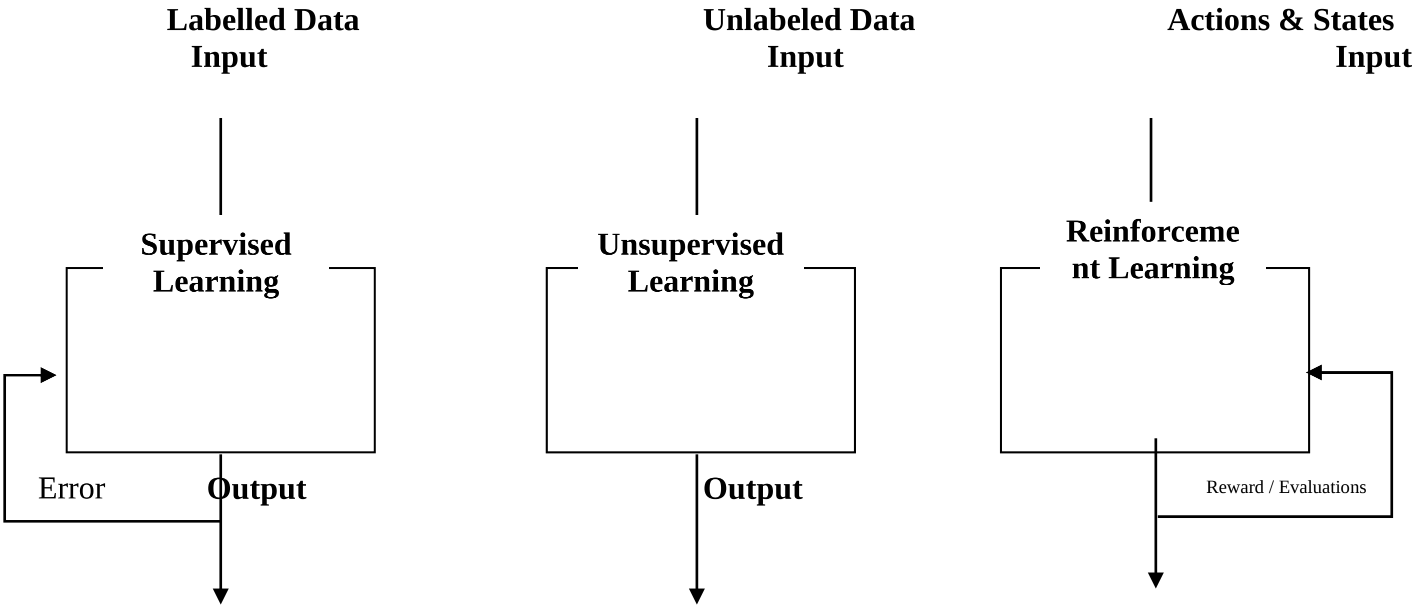


Figure 4 Types of Machine Learning

4.1 Related Work

Machine Learning has highly influenced the researchers working in the field of VANET Architectures. A wide range of algorithms have been proposed and proven their efficiency in terms of various QoS like Throughput, Jitter and PDR under the aegis of Machine Learning.

Since Vehicle to Vehicle communication is a constant generator of data in terms of nodes, congestion, weather-information and a lot more, it gives a huge opportunity to work upon.

Machine Learning in VANET can help in many areas, the taxonomy below lists them precisely. [31]

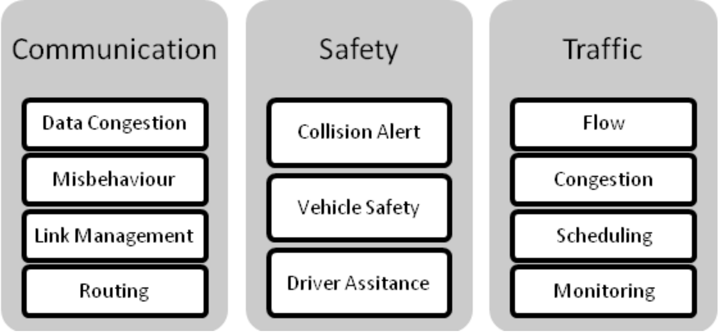


Figure 5 ML's areas of assistance in VANET

[32] Discusses at length about various algorithms of VANET under various categories like Fog Computing, ID Based, Clustering, Signature Based and Machine Learning. An extensive work has been discussed by [33] [25][31] [20]wherein the algorithms using Machine Learning have been discussed and a contrast has been displayed amongst the works.

[34][35][36] have used Support Vector Machine (SVM) and have shown the tremendous improvement up to 97% as compared to the previous work. These algorithms work upon DDOS, Probing and Misbehaviour. [37] used Artificial Neural Network (ANN) over NGSIM dataset on MATLAB and showed 99% accuracy under VANET. A jamming attack detection model has been proposed by [38] using unsupervised ML. It used K-means clustering on the generated dataset over VANET.

[25] used Binary and Multi Class Accuracy to find out the pattern of misbehaviour over the network. Various experiments proved that Random Forest and J-48 classifiers behaved much better compared to the rest of the classifiers used in the proposed work.

[24] used KNN and SVM to create a model for detecting and classifying the location spoofing misbehaviour.

5 Motivation & Proposed Methodology

The models discussed in the previous sections have used the concepts of Machine Learning very efficaciously. This work is highly inspired by the researchers who have contributed in the formation of a secured environment for Vehicle to Vehicle Communication. This paper aims at extending the work proposed by [39]. The referred work provides a mechanism to segregate the given simulation data into trusted and un-trusted nodes using a hybrid model comprising of Clustering and Ad-Hoc Distance Vector AODV over VANET. The algorithm has worked upon a Route Discovery Process using Cluster Head and Communication Centre which further adds on to the efficiency of the network by reducing overhead. This paper aims at categorising the simulation data into various clusters on the basis of their behaviour. Further we apply SVM and Feed Forward Back Propagation to see the efficiency of the proposed work. The overall work has been divided into three major segments and Section 6 shows the result of the proposed model.

5.1 Clustering is an unsupervised learning mechanism wherein the data is grouped into various clusters on the basis of their similarity with each other and dissimilarity with the data in the other clusters.

Here, we have used **Enhanced K- Means Clustering Algorithm** to make the clusters of the simulated dataset on the basis of Throughput, Jitter and PDR. The detailed algorithm has been explained as below:

```
Algorithm Enhanced K − Mean Clustering
Input: Sample Dataset(DS) − $\{A_i, B_i \dots, N_i\}$, K − Number of Clusters , N- Number of tuples
Output: A set of K number of Cluster
//In this case, DS is the dataset generated with the help of Matlab which comprises of three QoS as attributes on the basis of which the clusters are to be made namely Throughput, Jitter and PDR. We propose an Enhanced Version of K-Mean Partitioning Algorithm for clustering which does not take the centroid arbitrarily but with a said logic. Here, we take K as 3, as we will be working on three types of attacks and each cluster will be categorized on one of the attack.

1. Calculate the average of each attribute and denote it as a First Centroid($Cn_1$) of the cluster
   $Cn_1 = \left\{\frac{(A_1, A_2, \dots A_n)}{n}, \frac{(B_1, B_2, \dots B_n)}{n}, \dots \frac{(C_1, C_2 \dots C_n)}{n}\right\}$
2. Calculate the Second Cenroid ($Cn_2$)and Third Centroid($Cn_3$) with a random variation in the first centroid
3. Calculate the Euclidean Distance of each tuple with $Cn_1$, $Cn_2$ and $Cn_3$.
4. For i = 1:N
       a) For j=1:3 //Distance of every tuple is calculated with each of the three Centroid is calculated//
              Euclidean Distance $d_{ij} = \sqrt[2]{(ACn_j - A_i)^2 + (BCn_j - B_i)^2 + (CCn_j - C_i)^2}$
       b) end
           c) Find the minimum distance of each tuple with the three centroids
           d) (re)assign each tuple to the cluster with which it has the least distance
           e) recalculate the new centroid after the new additions/deletions to the cluster
5. until, no change
6. End
7. Return the three Clusters with the associated tuples
```

5.2 **Cluster Labelling** Once the clusters have been made with the help of Enhanced K-Means method, the next step is to label the clusters with the type of attacks. The proposed architecture deals with multiple attacks. Section III has listed all the major categorisation of the attacks and it clearly gives a contrast that DDoS attack is the most impactful one followed by Replay. Therefore, this algorithm works on these two attacks and the third one is Sybil attack which again would be dealt with in the proposed architecture.

To categorise the three attacks, we have used Mean Squared Error (MSE) to find out the correlation amongst the cluster elements. MSE is calculated for each of the cluster. The cluster with maximum MSE is labelled as DDoS class whereas the second one is labelled as Replay and the remaining one is labelled as Sybil attack. The following algorithm depicts the process of labelling the clusters.

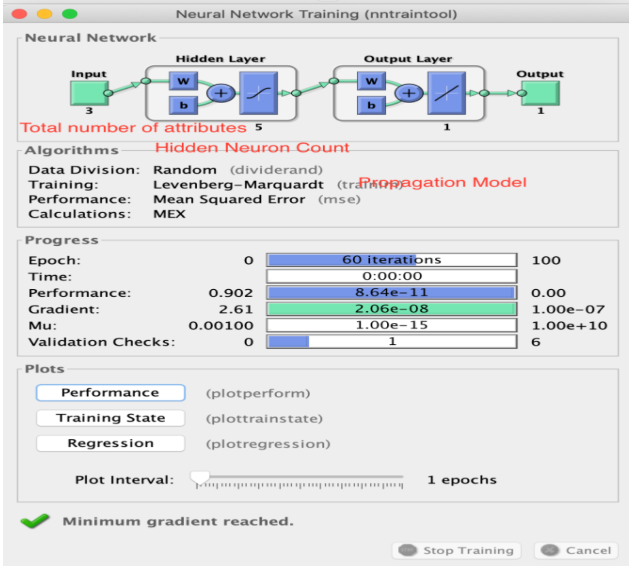
Algorithm ***To classify and label the clusters into various attacks***

```
Input:  Clusters with the sample data of routing nodes
Output: Labelled Clusters with the name of attacks.
// The input cluster carry three attributes which are Throughput, PDR and Jitter . Further, the algorithm
focuses on three types of attacks namely DDOS, Replay and Sybil and the three supplied clusters are
categorized accordingly
    1. Start
       //Compute the Mean Square Error (MSE)for all the clusters
    2. For i=1:3
           $\mathrm{MSE} = \frac{1}{n}\sum_{n}^{1} Y_i - \hat{Y}_i$
           where, n is  the number of data points
           $Y_i$ repesents the observed values
           $\hat{Y}_i$ repesents the predicted values
    3. For End
    4. Cluster with  maximum MSE → DDOS
    5. Cluster with  second highest MSE →Replay
    6. The third cluster is labeled as Sybil
    7. Return Labeled Clusters
```

6 Applying Machine Learning and Comparing with previous work

In this section, we will apply Machine Learning to the results derived with the proposed algorithm and to assess the efficiency of the proposed model. Machine Learning has two prominent approaches namely Supervised and Unsupervised learning. Both of them have proved their efficacy in various fields. The categorization and various algorithms have been discussed in the subsequent sections. As discussed, the supervised learning works on huge volume of labeled data which is intricate and not always possible to collect in real time scenarios. This challenge is dealt by providing a model with the features of both Supervised and Unsupervised Learning and is named as Semi-Supervised approach.

In our research we have used Artificial Neural Network to train the model. The model has been trained using NN training tool of MATLAB. The simulated data has been passed into the input layer of ANN. The network has used multiple hidden layers to process the results. Levenberg-Marquardt is used as propagation behaviour model. In every iteration the MSE is calculated as root node validation and is back propagated to the network. Linear regression is used for cross validation. Figure 6 shows the Training Structure of ANN.

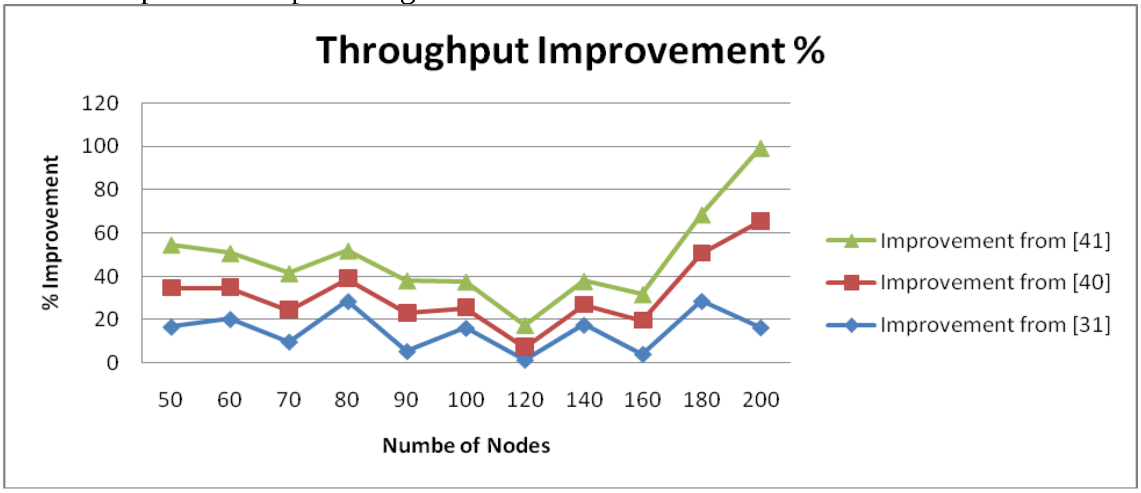


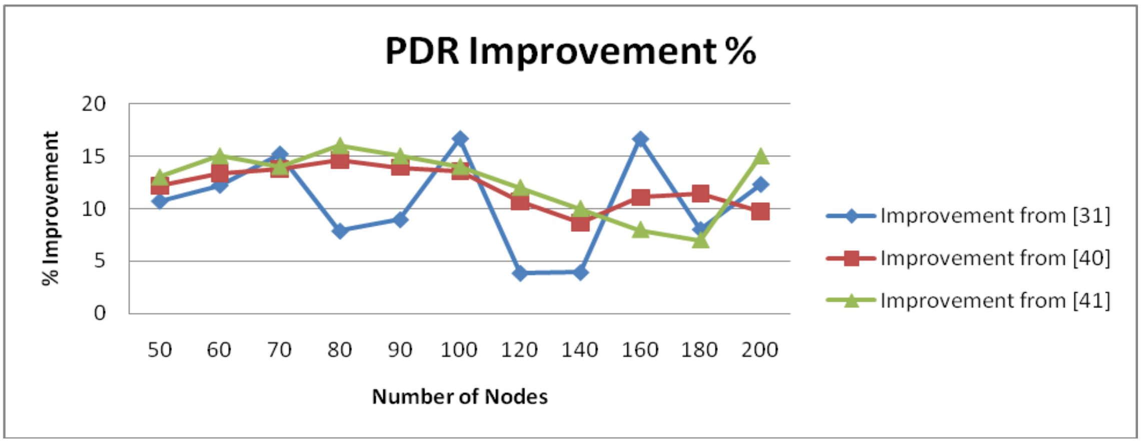
```
Neural Network Training (nntraintool)
Neural Network
        Input      Hidden Layer              Output Layer         Output
          3                       5                        1         1
Total number of attributes
Hidden Neuron Count
Algorithms
Data Division:   Random  (dividerand)
Training:        Levenberg-Marquardt  (trainlm)      Propagation Model
Performance:     Mean Squared Error  (mse)
Calculations:    MEX
Progress
Epoch:                    0    60 iterations     100
Time:                            0:00:00
Performance:          0.902      8.64e-11        0.00
Gradient:              2.61      2.06e-08        1.00e-07
Mu:                 0.00100      1.00e-15        1.00e+10
Validation Checks:        0          1           6
Plots
Performance      (plotperform)
Training State   (plottrainstate)
Regression       (plotregression)
Plot Interval:                    1 epochs
✓ Minimum gradient reached.
```

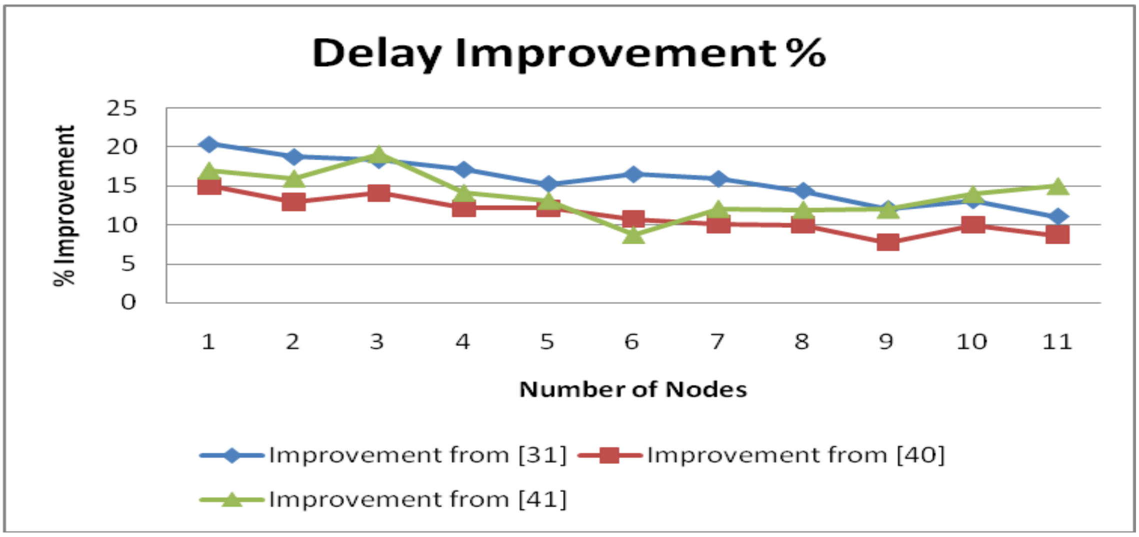
Figure 6 Training Structure of ANN.

7 Result

This section explains the results of the proposed algorithm when compared with the previous algorithms [40][31][41]. As discussed in the previous sections three QoS have been observed in the proposed research work namely throughput, PDR and Jitter. The improvement percentage in the results of the proposed algorithm has been depicted with the help of the graphs shared below. In all the three parameters it is inevitable that proposed algorithm has outperformed all the three base work algorithms.







Confusion Matrix

	D-DoS	Replay	Sybil	Total number of records	TPR	FPR
D-DoS	3358	122	108	3588	0.935897436	0.064102564
Replay	15	2406	27	2448	0.982843137	0.017156863
Sybil	19	23	3722	3964	0.938950555	0.010595358
				10000	0	

8 Conclusion & Future Work

In this paper, architecture has been proposed for disseminating information on VANET using AODV protocol with infused K-MEANS to apply Clustering on the data. Using Neural Network and SVM, the architecture has been trained to produce improved results. The proposed algorithm not only saves the network from DoS related attacks but also from Sybil and Replay. The results shown in the previous section prove the efficiency of the proposed algorithm in terms of QoS Jitter, PDR, TDR and Throughput when compared with the existing protocols [40][31][41]

In the future work, we are planning to explore in the following areas:

a. An algorithm which takes care of multiple attacks and not just DoS, Sybil and Replay

b. A variation to this algorithm can be looked at using SVM, Bagging and Bootstrap instead of Neural Network

c. Swarm Intelligence can also be applied for classification to get improved results

d. Hybrid Approach – using two or more approaches

e. According to the Linear Separability, the data can be checked and according to the co-variance & variance the technique can be chosen

f. Optimization techniques can be tried wherein the focus can be put upon the Feature Selection and Feature Reduction

9 Nomenclature

The following abbreviations are used in this paper:

ABC	Artificial Bee Colony
ANN	Artificial Neural Network
AODV	Ad-Hoc Distance Vector

CBLR	Cluster Based Location Routing
DoS	Denial of Service
FFBPNN	Feed forward back propagation neural network
HDSA	Hybrid DoS Attacks
ILA	Illusion Attack
ITS	Intelligent Transportation System
LTP	Long Term Pseudonym
MANET	Mobile Ad Hoc Network
MiMA	Man in the Middle Attack
ML	Machine Learning
MSE	Mean Squared Error
PDR	Packet Delivery Ratio
QoS	Quality of Service
RSU	Road Side Unit
SNI	Smart & Normal Intrusions
SVM	Support Vector Machine
TDR	True Detection Ratio
VANET	Vehicular Ad-hoc Network
VFC	VANET-cloud and fog computing
VFC	Vehicular Fog Computing

10. REFERENCES

1. M. Sharma and H. Khanna, "Issue 12 www.jetir.org (ISSN-2349-5162) JETIREC06080 Journal of Emerging Technologies and Innovative Research (JETIR) www.jetir," 2018. Accessed: Mar. 21, 2021. [Online]. Available: www.jetir.org.
2. "GLOBAL STATUS REPORT ON ROAD SAFETY 2018 SUMMARY," 2018. Accessed: May 24, 2021. [Online]. Available: http://apps.who.int/bookorders.
3. S. Tanwar, J. Vora, S. Tyagi, N. Kumar, and M. S. Obaidat, "A systematic review on security issues in vehicular ad hoc network," *Secur. Priv.*, vol. 1, no. 5, p. e39, Sep. 2018, doi: 10.1002/spy2.39.
4. [4] M. S. Al-Kahtani, "Survey on security attacks in Vehicular Ad hoc Networks (VANETs)," 2012, doi: 10.1109/ICSPCS.2012.6507953.
5. Deeksha, A. Kumar, and M. Bansal, "A review on VANET security attacks and their countermeasure," in *4th IEEE International Conference on Signal Processing, Computing and Control, ISPCC 2017*, Sep. 2017, vol. 2017-Janua, pp. 580–585, doi: 10.1109/ISPCC.2017.8269745.
6. M. H. Junejo *et al.*, "A Privacy-Preserving Attack-Resistant Trust Model for Internet of Vehicles Ad Hoc Networks," 2020, doi: 10.1155/2020/8831611.
7. M. A. Ahmed Shoeb Al Hasan, Md. Shohrab Hossain, "Security threats in vehicular ad hoc networks," 2016, doi: 10.1109/ICACCI.2016.7732079.
8. J. Domingo-Ferrer and Q. Wu, "Safety and privacy in vehicular communications," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2009, vol. 5599, pp. 173–189, doi: 10.1007/978-3-642-03511-1_8.
9. C. L. Chen, I. C. Chang, C. H. Chang, and Y. F. Wang, "A secure ambulance communication protocol for VANET," *Wirel. Pers. Commun.*, vol. 73, no. 3, pp. 1187–1213, 2013, doi: 10.1007/s11277-013-1273-y.
10. M. Barua, X. Liang, R. Lu, and X. Shen, "RCare: Extending secure health care to rural area using VANETs," *Mob. Networks Appl.*, vol. 19, no. 3, pp. 318–330, 2014, doi:

10.1007/s11036-013-0446-y.

11. V. Manjula and C. Chellappan, “The replication attack in wireless sensor networks: Analysis and defenses,” *Commun. Comput. Inf. Sci.*, vol. 132 CCIS, no. PART 2, pp. 169–178, 2011, doi: 10.1007/978-3-642-17878-8_18.
12. S. Bittl, A. A. Gonzalez, M. Myrtus, H. Beckmann, S. Sailer, and B. Eissfeller, “Emerging attacks on VANET security based on GPS Time Spoofing,” *2015 IEEE Conf. Commun. NetworkSecurity, CNS 2015*, pp. 344–352, 2015, doi: 10.1109/CNS.2015.7346845.
13. K. R. Malla, Adil Mudasir, “Security Attacks with an Effective Solution for DOS Attacks in VANET Security Attacks with an Effective Solution for DOS Attacks in VANET,” no. November, 2015, doi: 10.5120/11252-6467.
14. M. H. Junejo *et al.*, “A Privacy-Preserving Attack-Resistant Trust Model for Internet of Vehicles Ad Hoc Networks,” 2020, doi: 10.1155/2020/8831611.
15. T. Pavithra and B. S. Nagabhushana, “A Survey on Security in VANETs,” in *Proceedings of the 2nd International Conference on Inventive Research in Computing Applications, ICIRCA 2020*, Jul. 2020, pp. 881–889, doi: 10.1109/ICIRCA48905.2020.9182823.
16. S. Kofi and K. M. Elleithy, “Secure intelligent vehicular network using fog computing,” *Electron.*, vol. 8, no. 4, 2019, doi: 10.3390/electronics8040455.
17. J. Rupareliya, S. Vithlani, and C. Gohel, “Securing VANET by Preventing Attacker Node Using Watchdog and Bayesian Network Theory,” *Procedia Comput. Sci.*, vol. 79, pp. 649–656, 2016, doi: 10.1016/j.procs.2016.03.082.
18. S. Garg and G. S. Aujla, “An attack tree based comprehensive framework for the risk and security assessment of VANET using the concepts of game theory and fuzzy logic,” *J. Emerg. Technol. Web Intell.*, vol. 6, no. 2, pp. 247–252, 2014, doi: 10.4304/jetwi.6.2.247-252.
19. L. Liang, H. Ye, and G. Y. Li, “Toward Intelligent Vehicular Networks: A Machine Learning Framework,” Apr. 2018, doi: 10.1109/JIOT.2018.2872122.
20. A. M. Alrehan and F. A. Alhaidari, “Machine Learning Techniques to Detect DDoS Attacks on VANET System: A Survey,” *2nd Int. Conf. Comput. Appl. Inf. Secur. ICCAIS 2019*, pp. 1–6, 2019, doi: 10.1109/CAIS.2019.8769454.
21. G. E. P. Box and G. C. Tiao, “Bayesian inference in statistical analysis,” p. 588, 1992, Accessed: Nov. 15, 2021. [Online]. Available: https://www.wiley.com/en-in/Bayesian+Inference+in+Statistical+Analysis-p-9780471574286.
22. R. Jiang, C.-T. Li, D. Crookes, W. Meng, and C. Rosenberger, Eds., *Deep Biometrics*. Cham: Springer International Publishing, 2020.
23. J. Han, M. Kamber, and J. Pei, “Data Mining. Concepts and Techniques, 3rd Edition (The Morgan Kaufmann Series in Data Management Systems),” 2011.
24. S. So, P. Sharma, and J. Petit, “Integrating Plausibility Checks and Machine Learning for Misbehavior Detection in VANET,” *Proc. - 17th IEEE Int. Conf. Mach. Learn. Appl. ICMLA 2018*, pp. 564–571, Jan. 2019, doi: 10.1109/ICMLA.2018.00091.
25. J. Grover, N. K. Prajapati, V. Laxmi, and M. S. Gaur, “Machine learning approach for multiple misbehavior detection in VANET,” *Commun. Comput. Inf. Sci.*, vol. 192 CCIS, no. PART 3, pp. 644–653, 2011, doi: 10.1007/978-3-642-22720-2_68.
26. T. Kanungo, D. M. Mount, N. S. Netanyahu, C. D. Piatko, R. Silverman, and A. Y. Wu, “An efficient k-means clustering algorithms: Analysis and implementation,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 24, no. 7, pp. 881–892, Jul. 2002, doi: 10.1109/TPAMI.2002.1017616.
27. Y. W. Teh, “Dirichlet Process Motivation and Background.”
28. L. Rokach and O. Maimon, “DATA MINING WITH DECISION TREES,” Accessed: Nov. 15, 2021. [Online]. Available: http://www.worldscientific.com/series/smpai.
29. R. S. Sutton and A. G. Barto, “Reinforcement Learning: An Introduction Second edition, in progress.”

30. C. Weng, D. Yu, S. Watanabe, and B. H. F. Juang, "Recurrent deep neural networks for robust speech recognition," *ICASSP, IEEE Int. Conf. Acoust. Speech Signal Process. - Proc.*, pp. 5532–5536, Jan. 2014, doi: 10.1109/ICASSP.2014.6854661.
31. S. Khatri *et al.*, "Machine learning models and techniques for VANET based traffic management: Implementation issues and challenges," *Peer-to-Peer Netw. Appl. 2020 143*, vol. 14, no. 3, pp. 1778–1805, Sep. 2020, doi: 10.1007/S12083-020-00993-4.
32. H. Khanna, M. Sharma, and D. Rattan, "Secure and Authenticated Protocols for VANETs," 2021.
33. D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs)," *Veh. Commun.*, vol. 25, p. 100247, 2020, doi: 10.1016/j.vehcom.2020.100247.
34. M. Kim, I. Jang, S. Choo, J. Koo, and S. Pack, "Collaborative security attack detection in software-defined vehicular networks," *undefined*, pp. 19–24, Nov. 2017, doi: 10.1109/APNOMS.2017.8094172.
35. W. Li, A. Joshi, and T. Finin, "SVM-CASE: An SVM-based Context Aware Security Framework for Vehicular Ad-hoc Networks."
36. Y. Yu, L. Guo, Y. Liu, J. Zheng, and Y. Zong, "An efficient SDN-Based DDoS attack detection and rapid response platform in vehicular networks," *IEEE Access*, vol. 6, pp. 44570–44579, Jul. 2018, doi: 10.1109/ACCESS.2018.2854567.
37. F. A. Ghaleb, A. Zainal, M. A. Rassam, and F. Mohammed, "An effective misbehavior detection model using artificial neural network for vehicular ad hoc network applications," *2017 IEEE Conf. Appl. Inf. Netw. Secur. AINS 2017*, vol. 2018-January, pp. 13–18, Jul. 2017, doi: 10.1109/AINS.2017.8270417.
38. D. Karagiannis and A. Argyriou, "Jamming attack detection in a pair of RF communicating vehicles using unsupervised machine learning," *undefined*, vol. 13, pp. 56–63, Jul. 2018, doi: 10.1016/J.VEHCOM.2018.05.001.
39. H. Khanna and M. Sharma, "A Packet Efficient Architecture for Vanet Based on AODV and Clustering," in *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Jul. 2021, pp. 01–07, doi: 10.1109/ICCCNT51525.2021.9579852.
40. A. Ahamed and H. Vakilzadian, "Impact of Direction Parameter in Performance of Modified AODV in VANET," *J. Sens. Actuator Networks 2020, Vol. 9, Page 40*, vol. 9, no. 3, p. 40, Sep. 2020, doi: 10.3390/JSAN9030040.
41. K. J. Singh and T. De, "Efficient Classification of DDoS Attacks Using an Ensemble Feature Selection Algorithm," *J. Intell. Syst.*, vol. 29, no. 1, pp. 71–83, Jan. 2020, doi: 10.1515/JISYS-2017-0472/MACHINEREADABLECITATION/RIS.