International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-5, March 2020

Decision Tree and Neural Network Based Hybrid Algorithm for Detecting and Preventing Ddos Attacks in VANETS

Kaushik Adhikary, Shashi Bhushan, Sunil Kumar, Kamlesh Dutta

***Abstract*: The demand of Vehicular Adhoc Networks (VANETs) has been increasing in the area of vehicular and infrastructure communications. It has been felt that there is requirement of sharing of critical information related to safety and traffic management among different types of vehicles in a secure way. To ensure the smooth operation of the network, the availability of network resources is needed. The presence of either malicious vehicles or inaccessibility of network services makes VANET easy target for denial of service (DoS) attacks. The sole purpose of DoS attacks is to prevent the intended users from accessing the available resources and services. When the DoS attack is carried out by multiple vehicles distributed throughout the network, it is referred as Distributed DoS (DDoS) attack. The DDoS attacks are very dangerous and hard to be addressed in real time. The machine learning based DDoS attack detection algorithms have been proposed and presented by the research community in literature. In this paper, a hybrid algorithm of Decision Tree and Neural Network is presented for detecting and preventing different types of DDoS attacks in VANETs with highly efficient results. The simulation based experiments are carried out in order to evaluate and compare the performance of proposed hybrid algorithm with respect to different performance parameters. Based on experiments results, it has been found that the performance of hybrid algorithm has been increased significantly*.

***Keywords:** VANETs, DDoS attack, decision tree, neural network, machine learning algorithm, hybrid model etc.*

I. INTRODUCTION

The indigenous desire of humans for entertainment, safety, mobility and security has led to the evolution of vehicular from some mere mechanical locomotives to Intelligent Transportation Systems (ITS). Vehicular Adhoc Networks (VANETs) has been found to be the most suitable technology for ITS [1]. These networks are generally formed for a short duration by the vehicles possessing wireless communication capability. These vehicles are equipped with On Board Unit (OBU). These units are electronic devices which can interact with other vehicles (V-V communication) equipped with OBUs as well as with Road Side Units (RSUs) (V-I communication) using short range direct communications as shown in Fig.1. The Road Side Units play the role of infrastructure based communication. The real time scenario of the condition of a road is gained from vehicles, CCTVs, sensors and RSUs. All the information gained from various sources are analyzed by OBUs and final scenario is presented to the users. The different types of information generated through various sources can lead to the creation of different types of real time applications catering to different needs. So, various types of ITS related projects are continuously coming up and are being encouraged to be undertaken by various ITS stakeholders such as governments, organizations and vehicle manufacturers. In India, due to the digital revolution the Government of India has recognized the need for building innovative transport networks[2].

The modern vehicles are equipped with various features like remote locking, high speed alerts, rear parking sensors, airbags etc. But, these features are being provided without keeping their security in mind. The main focus of developing VANETs is providing safety to human lives. These networks are just modification of Mobile Adhoc Networks (MANETs) with typical features such as unlimited battery power, predictable vehicular movements, infotainments etc. The applications which provide safety related information should be secured from malicious vehicles as any compromise in the safety and security of these applications can lead to death of living beings which are communicating on the track. Without security features in VANETs, it can lead to different types of attacks like Denial of Service Attacks (DoS), message suppression, spreading of false alerts which finally results to any type of accidents. When the DoS attack is carried out by multiple vehicles distributed throughout the network, it is referred as Distributed DoS (DDoS) attack. The DDoS attacks are very dangerous and hard to be addressed in real time.

Revised Manuscript Received on March 30, 2020.
* Correspondence Author
Kaushik Adhikary*, Computer Science and Engineering, I.K.Gujral Punjab Technical University, Kapurthala, India. Email:kaushik.nith@gmail.com
Shashi Bhushan, Computer Science and Engineering, Chandigarh Group of Colleges, Landran, India. shashibhushan6@gmail.com
Sunil Kumar, Computer Science and Engineering, Maharaja Agrasen University, Baddi, India. Email: sunilkaushik27@gmail.com
Kamlesh Dutta, Computer Science and Engineering, National Institute of Technology, Hamirpur, India. Email: kdnith@gmail.com

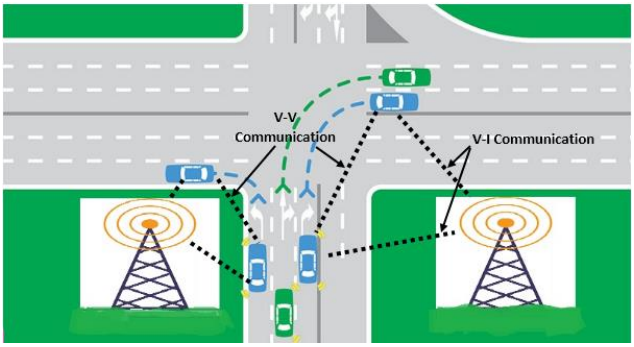

Fig.1. Communications carried out in a VANET setup

The ultimate goal of VANETs can only be achieved if its services are seamlessly available to all its intended users. Any minor disruption in its functioning / service can create a major havoc in the lives of human commuters depending on its services. One of the instance that is cited here in Fig. 2 where a car is travelling on a slope in a foggy environment in a mountain area, and there is a sharp curve ahead.

Fig.2. A car on a foggy weather driving on a mountain

In the above cited case, user / driver is fully dependent on the service of VANETs. Due to any miscellaneous reason, the service of VANET may become unavailable. This situation can create a horrible scenario because driver is not able to see the sharp curve ahead without the service of VANETs and may be go down the mountain leading to loss of his / her life.

The scenario described above is the case where unavailability of the service of VANET leads to loss of human life. If such type of scenario is caused intentionally by any malicious user on the network than this attack is known as a DoS attack wherein the main objective of attacker is to make the unavailability of services of a network to its intended users.

The presence of either malicious vehicles or inaccessibility of network services makes VANET easy target for denial of service (DoS) attacks. The sole purpose of DoS attacks is to prevent the intended users from accessing the available resources and services. One of the easy technique of a DoS attack is to make a service unavailable to the users by flooding the network with bogus packets and consuming the network resources like memory, processor, bandwidth etc. When the DoS attack is carried out by multiple vehicles distributed throughout the network, it is referred as Distributed DoS (DDoS) attack. The DDoS attacks are very dangerous and hard to be addressed in real time.

There is a requirement for developing an effective defensive mechanism which can differentiate among the flow of normal traffic vs the malicious traffic. It is a general presumption that whenever there is a high volume of traffic or high packet drop, the network is under attack [3][4]. There is no predefined structure of a normal traffic flow. Detection techniques based on single machine learning models have high accuracy but they suffer from making error on different training dataset[5]. So, by combining their predicted value, this error can be reduced and their accuracy can be improved even on a miscellaneous data set. The idea is to develop a hybrid model that is as varied as possible and combining the predicted value of machine learning models for the accurate detection decisions.

The hybrid approach presented here is similar to that described in [6] where authors gave main focus on combining the best features of Decision tree and Neural Networks in order to deliver the highly efficient Intrusion detection system. In [6], authors presented hybrid approach by first employing Neural Networks and their after Decision tree in order to increase the intrusion detection rate over KDD Cup 99 dataset whereas the hybrid approach presented in this paper employs first Decision tree and their after Artificial Neural Networks in order to increase the detection accuracy over simulated dataset for VANET environment. Basically, the hybrid approach presented here is inspired from the work of Sindhu, Geetha, and Kannan [6]. Even, the algorithm DecineuralModel presented in this paper is similar to algorithm Neurotree in [6].

Decision trees belong to supervised learning algorithms. They are commonly used for regression and classification problems. Decision trees are classified as a regression tree and a classification tree according to the nature of the problem. IDS methods using decision trees were used in [6]–[9] to achieve the best detection results. The decision tree consists of the root (start node), branching nodes (decision nodes) and terminal nodes (end nodes). The tree is built step by step, starting with finding the only variable that can divide the data into two parts. The process is repeated for sub parts and continues until a minimum size is obtained or further separation is not possible. Decision nodes are connected to their ancestors and descendants through the edges. The end nodes are called leaves, which indicate the final decision. Leaves are classified according to class labels. Basically, Decision trees are used for classification.

Artificial Neural Networks (ANNs) are based on the functioning of the human brain. They differ from the conventional classification algorithms, since the structure of a neural network (known as a neuron) is able to obtain knowledge from its experience, which makes it very suitable for understanding unknown patterns [10]. ANN consists of an input layer, one or more hidden layers and an output layer. Various types of ANNs can be created, such as single layer, multi-layer, direct connection, back propagation, etc. [11]. Like the human brain, ANN consists of a large number of interconnected processor elements that transform a set of input data into a preferred set of output data [12]. This result is obtained by the characteristics of weights and elements. By changing the values of these weights and elements, desired result can be obtained. This feature of ANN makes it applicable to various problems. ANN learns from its experience, which makes it very flexible to learn new problems. ANN can also learn from incomplete data and has the ability to analyze data from the network. A natural way to solve the problem is also a major advantage of ANN.

The main objective of this paper is to propose an effective hybrid algorithm which can detect different types of DDoS attacks (known as well as unknown attacks) with in very short time as they begin to exhibit their malicious behavior. The results obtained throughout the simulation experiments clearly show that the proposed hybrid approach is practical to improve the malicious nodes detection accuracy, and capable to alleviate the impact of malicious nodes from the network.

The rest of the paper is structured as follows. Section 2 summarizes the related work. In Section 3, the relevant elements of the proposed hybrid approach are described. In Section 4, the results and analysis are presented. Finally, Section 5 concludes the proposed hybrid approach and provides the directions to future work.

II. RELATED WORKS

Several detection techniques have been proposed by research community in the literature to secure the VANETs from DDoS attacks [13]–[17].

In [18] the authors have focused on a single type of attack known as illusion attacks. In this type of attack, the attackers inject wrong information into the network. The authors have specified certain rules stored in a rule database and a checking module which can determine whether a particular message should be considered valid or not. The weakness with this approach is that as the rule are fixed, the attackers can easily manipulate their message to fulfil all the rules and avoid detection.

Authors in [19] used a trust based mechanism for detecting DDoS attacks. Using the strength of the existing Firecol based security procedure with Dynamic Growing Self organizing Tree Algorithm in the trust evaluation based environment, a trust evaluator matrix was formed which gave the lowest trust value to the attacker nodes. Evaluation of the proposed model was done on the basis of various security metrics and performance metrics. The weakness of this model is that it considers majority of vehicles as honest nodes.

In[20], the authors have used position based model which is focused on depicting a real world scenario where the pseudonyms are rapidly changing. For determining the position of the vehicles the authors have used Kalman Filter. This information is updated on receiving a message. This approach as claimed by the authors can increase the attack detection and also can be used for collision avoidance. The breach in privacy and somewhat higher computational cost are the main weakness of this approach.

The anomaly based techniques which are based on different machine learning techniques have been used extensively in literature for detecting DoS attacks. Many of these techniques are based on a single technique like genetic algorithm, neural networks, support vector machine etc. while many techniques use the combination of existing methods developing a hybrid [21].

Authors in [22] proposed a Deep Neural Network (DNN) approach to detect Intrusion in Vehicular Networks. The DNN consists of a number of hierarchical layers of non-linear stages of processing. The IDS approach using Deep Convolutional Neural Network (DCNN) was proposed in [23] for security in vehicle network. The dataset used for training the model as well as testing the model was obtained from a real vehicle.

The main aim of developing a detection algorithm to get the best accuracy. This aim has increased the need for developing algorithm based on hybrid approach. The hybrid approach combines different machine learning algorithm with the main objective to improve the system performance. The hybrid approach more precisely contains two different algorithms. The idea behind hybrid approach is to train a model on a raw data and obtain a result. This result is then sent to another model as input and get the final result. Hybrid approach have been used in [24]–[27]

III. PROPOSED HYBRID MODEL FOR DETECTING AND PREVENTING VANET FROM DDOS ATTACK

The hybrid algorithm proposed in this paper determines the behavior of a vehicle as normal or an attacker. The dataset produced by the simulation has both the normal and attacker behavior of a vehicle. The type of features used and their quantities play an important role in increasing the accuracy and decreasing the false positive ratio. The features which are highly relevant for DDoS attack are used in this paper for the simulation purpose have been done in previous study [12]. In this paper the Decision Trees and Neural network have been combined in designing the hybrid model as these techniques have been used earlier as discussed in the previous section.

The proposed hybrid technique attempts to provide an efficient detection model against known as well as unknown DDoS attacks that can take place in VANET environment. The simulation of the whole model was done on RStudio. The following describes the methodology used to carry the work.

A. Simulation of VANET

In the first step, VANET was simulated under normal condition and then under DDoS attack condition. The normal vehicles have their behavior set as 0 and the attacker vehicle as 1. The dataset obtained contained both the condition was stored in “data1.csv”. A critical step in simulation are the initial stages where the different simulation environment and their parameters are set. Table I gives the overview of this setup. As mentioned in the Table I, there are 1000 vehicles and 5 RSUs. Those vehicles which are in the range of a RSU create a VANET. The range of RSU has been set at 200 meters (m). There are 5 features set for each vehicle. Every normal vehicle has normal features. Some vehicles in each RSU have malicious features to simulate DDoS attack. The goal of this paper is to detect these attacker vehicles from normal vehicles.

Table- I: Simulation environment and their parameter

Simulation environment	Parameter
No. of Vehicles	1000
No. of RSUs	5
Topology	1000*1000 (m)
RSU network range	200(m)
Features	Collision, delay, jitter, packetdrop, ratioinout and throughput
Maximum no of packets sent by a vehicle	1000
Vehicle Speed	40-60m/s

B. Simulation of Existing Models

The dataset obtained in the first step are fed to the existing machine learning model for getting their prediction values. The machine learning algorithms used here are Decision Tree, Neural Network, SVM with RBF dot kernel, Linear Model and Random Forest. The logic behind using the existing model is to obtain the actual behavior of the vehicle by using the Voting Method. In the voting method the maximum number of count of an instance is taken as the actual value. For ex. if out of 5 models, 3 are predicting a vehicle as 0 then the actual value is taken as 0. The actual behavior of the vehicle is used for evaluating the proposed hybrid algorithm. The Table II shows the voting method technique. This data is stored in "data2.csv".

C. Simulation of Hybrid Algorithm

The proposed hybrid algorithm is designed using the Chaining method [28]. In this method the inputs of a dataset are used for training a model. The predictions obtained by this training along with initial input are used for training the second model. In this paper first the inputs are used for training the Decision Tree. The predictions obtained from training the Decision Tree along with the initial inputs are used for training the Neural Network.

D. Evaluating the Proposed Hybrid Algorithm

The predictions obtained from the proposed Hybrid technique is compared with the Actual value obtained in the 2nd stage. The model is then evaluated on the parameters: H, Gini, AUC, AUCH, KS, MER, TPR, FPR and Accuracy and compared the performance with the existing techniques: Decision Trees and Neural Network. The result and analysis is discussed in the next section.

IV. RESULT AND ANALYSIS

The core objective of this paper was to design an effective DDoS detection technique for providing a safe and secure environment for VANETs. This technique was implemented in 4 stages which lead to first obtaining the dataset containing normal as well as DDoS attack features, training and predicting different models for obtaining actual value, training and predicting the hybrid model based on the initial dataset and then evaluating the proposed hybrid model on the basis of different parameters: H, Gini, AUC, AUCH, KS, MER, TPR, FPR and Accuracy.

Table III-V shows the parametric values of 5 RSUs of Decision Tree, Neural Network and the proposed Hybrid Algorithm. The simulation has been done 5 times as the VANET model designed contained 5 RSUs.

The Table VI has been derived from Table III-V. In this table, the parameters contain the average of a parameter of 5 RSU. For ex. the H value of Decision Trees is obtained by averaging the H values of 5 RSUs of Table III. The Table VI gives the comparative performance of the models. As this Table VI shows that all the parametric values of the proposed Hybrid model have higher performance compare to the single models: Decision Trees and Neural Network. This shows that by combining both this models and creating a hybrid the performance of a detection model increases significantly.

Table VII shows the ranking given by TOPSIS. TOPSIS is a tool available in RStudio which gives the ranking to models based on their comparative performances. Here, all the parametric values of the models are fed to the TOPSIS and their ranking is obtained. As seen the Table VII, TOPSIS has given the highest rank to the proposed Hybrid Model. The score of the proposed hybrid model is significantly higher than the existing model: Decision Tree and Neural Network. Finally, Fig. 3 shows the performance of the models for 5 RSUs.

Table- II: The Voting Method

Vehicle No	Linear Model	Neural Network	Random Forest	SVM with RBF	Decision Trees	Actual
1	0	0	1	1	0	0
2	1	1	1	1	0	1
3	0	0	1	1	0	0
4	0	0	0	1	0	0
5	0	0	1	1	0	0
6	1	1	1	1	0	1
7	0	0	0	1	0	0
8	1	1	1	1	0	1
9	0	0	0	1	0	0
10	1	1	1	1	0	1

Table- III: Evaluation of Decision Trees

RSU	H	Gini	AUCH	KS	MER	TP	FP	TN	FN	TPR	FPR	Accuracy
1	0	0	0.5	0	0.31	0	0	44	95	0	0	31.65
2	0	0	0.5	0	0.29	0	0	82	196	0	0	29.5
3	0	0	0.5	0	0.26	0	0	112	305	0	0	26.86
4	0.77	0.89	0.94	0.89	0.07	351	0	165	40	0.89	0	92.81
5	0	0	0.5	0	0.28	0	0	195	500	0	0	28.06

Table- IV: Evaluation of Neural Network

RSU	H	Gini	AUCH	KS	MER	TP	FP	TN	FN	TPR	FPR	Accuracy
1	0.43	0.58	0.79	0.85	0.64	70	4	40	25	0.73	0.091	34.53
2	0.23	0.47	0.73	0.73	0.47	96	1	81	100	0.49	0.012	56.47
3	1	1	1	1	1	305	0	112	0	1	0	97.84
4	0.91	0.96	0.98	0.98	0.96	376	0	165	15	0.96	0	97.12
5	0.91	0.94	0.97	0.97	0.94	496	9	186	4	0.99	0.046	98.13

Table- V: Evaluation of Hybrid Model

RSU	H	Gini	AUCH	KS	MER	TP	FP	TN	FN	TPR	FPR	Accuracy
1	0.86	0.92	0.96	0.96	0.92	92	2	42	3	0.96	0.04	96.4
2	0.76	0.85	0.92	0.92	0.85	187	8	74	9	0.95	0.09	93.88
3	0.97	0.98	0.99	0.99	0.98	303	1	111	2	0.99	0.009	99.28
4	0.96	0.98	0.99	0.99	0.98	387	1	164	4	0.99	0.006	99.1
5	0.75	0.85	0.92	0.92	0.85	470	16	179	30	0.94	0.08	93.38

Table- VI: Comparative Performance of Proposed Hybrid Model with Existing Model

Models	H	Gini	AUC	AUCH	KS	MER	TPR	FPR	Accuracy
Decision Trees	0.15	0.17	0.58	0.58	0.17	0.24	0.17	0	41.77
Neural Network	0.70	0.79	0.89	0.90	0.80	0.11	0.83	0.02	76.81
Hybrid Model	0.86	0.92	0.96	0.96	0.92	0.03	0.96	0.04	96.40

Table- VII: Rank by TOPSIS

RANK	SCORE	MODEL
1	0.844896	Hybrid Model
2	0.71353	Neural Network
3	0.155104	Decision Trees

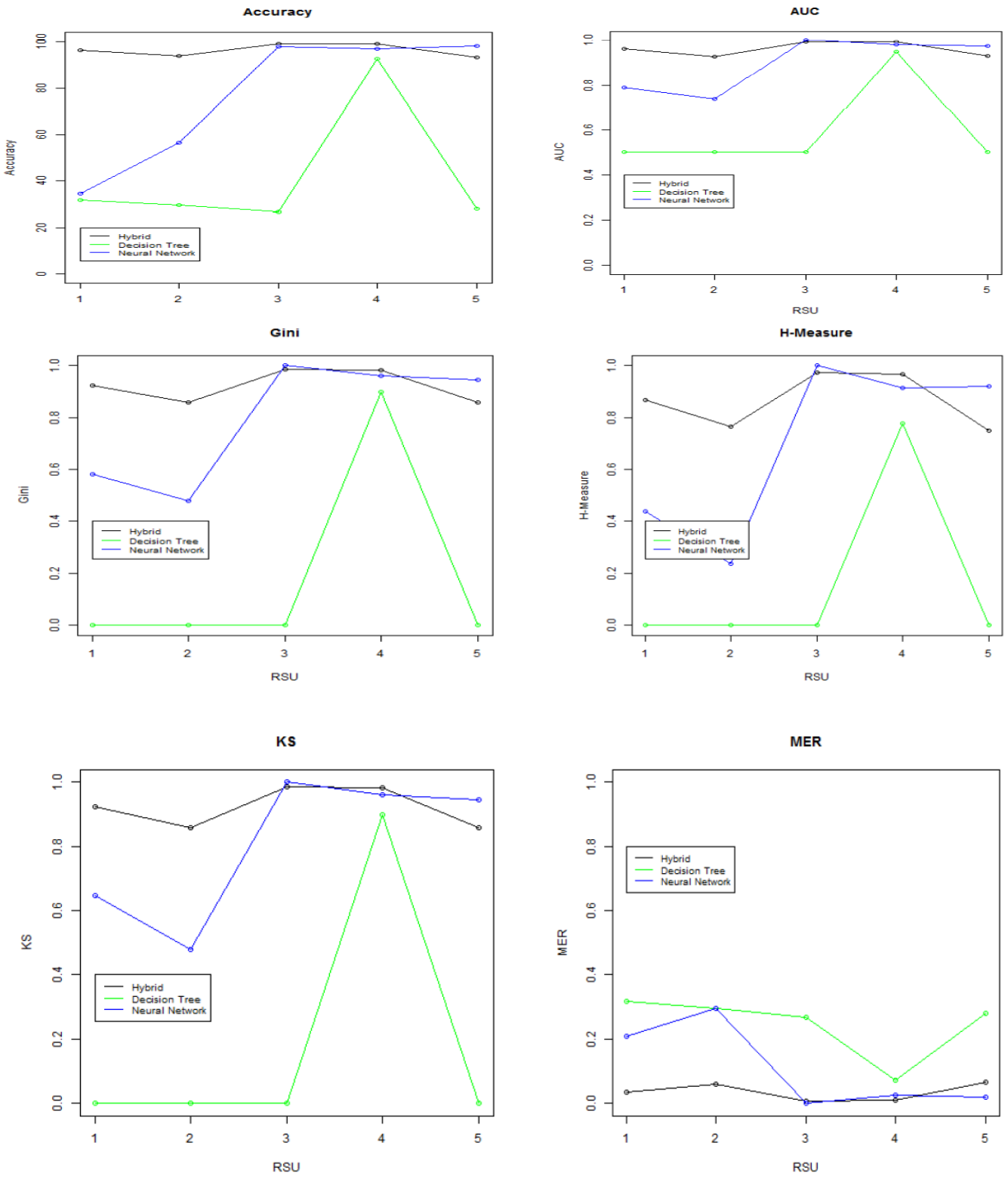

Fig.3. Evaluation of All the Models Based on Different Parameters for 5 RSUs

V. CONCLUSION

To make the VANET a successful technology, it is necessary to make it secure from DDoS attacks. The DDoS attacks are the most challenging problem that a VANET can face. It becomes a tough challenge to detect DDoS attack accurately and swiftly without affecting the normal traffic. The main objective of this research paper was to propose an efficient hybrid technique for detecting DDoS attacks which in turn can provide a safe driving for VANET. The proposed technique was implemented in 4 phases starting from simulating VANET, generating normal and malicious data, training and testing the existing technique as well as the proposed technique based on these data and finally

evaluating the proposed technique by comparing with existing techniques Decision Trees and Neural Network on various parameters. From these experimental results it has been found that the proposed hybrid technique has the best detection performance over the existing techniques.

REFERENCES

1. K. B. Kelarestaghi, M. Foruhandeh, K. Heaslip, and R. Gerdes, "Survey on Vehicular Ad Hoc Networks and Its Access Technologies Security Vulnerabilities and Countermeasures," 2019.
2. "Building innovative transport networks _ Business Standard Column." .
3. A. Quyoom, R. Ali, D. N. Gouttam, and H. Sharma, "A novel mechanism of detection of denial of service attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA)," in International Conference on Computing, Communication and Automation, ICCCA 2015, 2015.
4. L. Mokdad, J. Ben-Othman, and A. T. Nguyen, "DJAVAN: Detecting jamming attacks in Vehicle Ad hoc Networks," Perform. Eval., 2015.
5. P. A. Raj Kumar and S. Selvakumar, "Distributed denial of service attack detection using an ensemble of neural classifier," Comput. Commun., vol. 34, no. 11, pp. 1328–1341, 2011.
6. S. S. Sivatha Sindhu, S. Geetha, and A. Kannan, "Decision tree based light weight intrusion detection using a wrapper approach," Expert Syst. Appl., vol. 39, no. 1, pp. 129–141, 2012.
7. M. Kumar, M. Hanumanthappa, and T. V. S. Kumar, "Intrusion Detection System using decision tree algorithm," Int. Conf. Commun. Technol. Proceedings, ICCT, pp. 629–634, 2012.
8. K. Rai, D. M.Syamala, and A. Guleria, "Decision Tree Based Algorithm for Intrusion Detection," Int. J. Adv. Netw. Appl., vol. 7, no. 4, pp. 2828–2834, 2016.
9. C. Azad and V. K. Jha, "Decision Tree and Genetic Algorithm Based Intrusion Detection System," in Proceeding of the Second International Conference on Microelectronics, Computing & Communication Systems (MCCS 2017), 2019, pp. 141–152.
10. Z. Wu, L. Zhang, and M. Yue, "Low-Rate DoS Attacks Detection Based on Network Multifractal," IEEE Trans. Dependable Secur. Comput., vol. 13, no. 5, pp. 559–567, 2016.
11. I. Ahmad, A. B. Abdullah, A. S. Alghamdi, N. a Baykara, and N. E. Mastorakis, "Artificial neural network approaches to intrusion detection: a review," Telecommun. Informatics, no. January, pp. 200–205, 2009.
12. K. Adhikary, S. Bhushan, S. Kumar, and K. Dutta, "Evaluating the Performance of Various Machine Learning Algorithms for Detecting DDoS Attacks in VANETs," Int. J. Control Autom., vol. 12, no. 5, pp. 478–486, 2019.
13. V. Hoa La and A. Cavalli, "Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey," Int. J. AdHoc Netw. Syst., vol. 4, no. 2, pp. 1–20, 2014.
14. B. Mokhtar and M. Azab, "Survey on Security Issues in Vehicular Ad Hoc Networks," Alexandria Eng. J., vol. 54, no. 4, pp. 1115–1126, 2015.
15. H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," Veh. Commun., vol. 7, no. January, pp. 7–20, 2017.
16. L. Bariah, D. Shehada, E. Salahat, and C. Y. Yeun, "Recent advances in VANET security: A survey," in 2015 IEEE 82nd Vehicular Technology Conference, VTC Fall 2015 - Proceedings, 2016.
17. R. W. Van Der Heijden, S. Dietzel, T. Leinmüller, and F. Kargl, "Survey on misbehavior detection in cooperative intelligent transportation systems," IEEE Commun. Surv. Tutorials, vol. 21, no. 1, pp. 779–811, 2019.
18. N. W. Lo and H. C. Tsai, "Illusion attack on VANET applications - A message plausibility problem," GLOBECOM - IEEE Glob. Telecommun. Conf., 2007.
19. M. Poongodi and S. Bose, "A Novel Intrusion Detection System Based on Trust Evaluation to Defend Against DDoS Attack in MANET," Arab. J. Sci. Eng., vol. 40, no. 12, pp. 3583–3594, 2015.
20. H. Stubing, J. Firl, and S. A. Huss, "A two-stage verification process for Car-to-X mobility data based on path prediction and probabilistic maneuver recognition," IEEE Veh. Netw. Conf. VNC, pp. 17–24, 2011.
21. C. F. Tsai, Y. F. Hsu, C. Y. Lin, and W. Y. Lin, "Intrusion detection by machine learning: A review," Expert Syst. Appl., vol. 36, no. 10, pp. 11994–12000, 2009.
22. M. J. Kang and J. W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," PLoS One, vol. 11, no. 6, pp. 1–17, 2016.
23. H. M. Song, J. Woo, and H. K. Kim, "In-vehicle network intrusion detection using deep convolutional neural network," Veh. Commun., vol. 21, p. 100198, 2020.
24. J. Yao, S. Zhao, and L. Fan, "An Enhanced Support Vector Machine Model for Intrusion Detection," Rough Sets Knowl. Technol., pp. 538–543, 2006.
25. F. ALIAKBARI NOURI, S. KHALILI ESBOUEI, and J. ANTUCHEVICIENE, "A Hybrid MCDM Approach Based on Fuzzy ANP and Fuzzy TOPSIS for Technology Selection," Informatica, vol. 26, no. 3, pp. 369–388, 2015.
26. S. Sharma and A. Kaul, "Hybrid fuzzy multi-criteria decision making based multi cluster head dolphin swarm optimized IDS for VANET," Veh. Commun., vol. 12, 2018.
27. U. Ravale, N. Marathe, and P. Padiya, "Feature selection based hybrid anomaly intrusion detection system using K Means and RBF kernel function," Procedia Comput. Sci., vol. 45, no. C, pp. 428–435, 2015.
28. K. Zaamout and J. Z. Zhang, "Improving neural networks classification through chaining," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 7553 LNCS, no. PART 2, pp. 288–295, 2012.

AUTHORS PROFILE

Kaushik Adhikary is an Assistant Professor at Maharaja Agrasen University, Solan, India. He is currently pursuing PhD in the area of intrusion detection at I.K.Gujral Punjab Technical University, Jalandhar. He also holds Bachelor and Master's degrees in Computer Science And Engineering from NIT Hamirpur and Maharishi Markandeshwar University Mullana respectively. Kaushik Adhikary has published 15 research papers so far in various national, international journals and conferences.

Shashi Bhushan did his Ph.D from NIT, Kurukshetra, India in 2015. Dr. Bhushan is presently working as a HOD and Professor in department of Computer Science and Engineering at CEC, Landran since April 2011. He is having more than 18 years of academic and administrative experience. Dr. Bhushan has published more than 20 research papers in various National/International Journals of repute. His areas of interest are Peer to Peer Networks, Mobile Computing and Databases.

Sunil Kumar is at present working as Associate Professor at Maharaja Agrasen University, Baddi (Solan)-174103 (H.P.) India. He received his bachelor's degree in Computer Engineering from the Kurukshetra Univesrsity, Kurukshetra (India) in 2002 and master's degree in Computer Science and Engineering from Guru Jambheshwar University of Science and Technology, Hisar (India) in 2007. He has been awarded Gold Medal for standing first in 2005–2007 batch of Master of Technology in Computer Science and Engineering, Guru Jambheshwar University of Science and Technology, Hisar (India). He earned his Ph.D degree in Computer Science and Engineering from National Institute of Technology, Hamirpur (H.P.), India. His research interests include Wireless Networks and Information Security

Kamlesh Dutta is at present working as Associate Professor and Head of Computer Science and Engineering Department at National Institute of Technology, Hamirpur (H.P.), India. She earned her Ph.D. degree from Guru Gobind Singh Indraprastha University, Delhi (INDIA) and M.Tech. degree from Indian Institute of Technology, Delhi (India), and M.S. from Vladimir State University, Russia. Her major research interests include Artificial Intelligence, Network Security and Software Engineering. Seven students have completed their Doctorate under her guidance and other three are pursuing their Ph.D. under her. She has published more than 95 research papers in national and International Journals and Conferences. Quite a few of her technical papers have been awarded "Best paper award". She has chaired many national and international conferences and workshops. She reviews manuscripts on behalf of a large number of international journals.